

# 桃園縣政府 102 年使用個人資料防護研析專報



桃園縣政府政風處編撰

102 年 10 月 1 日

## 目 錄

壹、前言.....	1
貳、學說與學理之探討.....	2
一、個人資訊及隱私權的內容意涵：.....	2
(一) 個人資訊的取得、蒐集：.....	2
(二) 個人資訊的保有、管理、利用：.....	3
(三) 個人資訊之閱覽、訂正請求權：.....	3
二、隱私權的分類：.....	4
(一) 國外法制：.....	4
(二) 司法院大法官解釋：.....	5
參、現行法令規範及本府各機關行政程序：.....	6
一、個資法立法沿革：.....	6
二、個資法新法修正重點：.....	7
(一) 擴大保護客體及名稱之修正：.....	7
(二) 擴大適用主體及領域：.....	8
(三) 不定義主管機關：.....	8
(四) 新法排除適用範圍：.....	9
(五) 特種個人資料之蒐集、處理或利用：.....	9
(六) 蒐集、處理或利用資料前之告知義務：.....	9
(七) 增強個人資料當事人之權利：.....	10
(八) 明定一般資料之蒐集、處理及利用要件：.....	11
(九) 明定書面同意之定義：.....	13
(十) 強化行政監督：.....	13
(十一) 團體訴訟：.....	14
(十二) 相關責任：.....	14
三、本府各機關相關法令規定與行政流程：.....	16
(一) 警察局：.....	16
(二) 其他機關就戶役政資訊系統部分：.....	17
肆、本國與外國有關個人資料與資訊安全之維護措施：.....	19
一、我國有關個資資訊安全之維護措施：.....	19
二、外國有關個資資訊安全之維護措施：.....	19
(一) 歐美國家部分：.....	19
(二) 日本部分：.....	22
伍、可能易滋弊端態樣研析.....	26
一、公務部門案例類型：.....	26
(一) 查詢他人個資供己使用：.....	26
(二) 接受朋友請託代為查詢：.....	27

(三) 協助他人營利: .....	30
(四) 收售價金與業者合謀: .....	31
(五) 遭不法集團欺騙代為查詢: .....	33
(六) 以協辦業務之便取得系統權限: .....	34
(七) 提供關鍵資訊協助冒充警方人員: .....	35
(八) 藉洩漏個資之機索要財物與不法利益: .....	36
二、企業洩漏個資爭議事件: .....	37
陸、本府使用個人資料資訊系統專案稽核成果: .....	39
一、專案稽核概況: .....	39
(一) 專案稽核計畫: .....	39
(二) 受稽核機關(或單位): .....	39
(三) 稽核項目: .....	39
(四) 稽核人數: .....	39
(五) 稽核資料筆數: .....	40
(六) 發現缺失: .....	40
二、各機關專案稽核項目及稽核件(人)數: .....	40
(一) 本府地方稅務局: .....	40
(二) 本府衛生局: .....	41
(三) 本府警察局: .....	42
(四) 民政局: .....	43
(五) 地政局: .....	44
三、各機關專案稽核發現之相關缺失: .....	45
四、行政懲處或函送情形: .....	48
柒、策進措施與建議事項 .....	48
一、制度面: .....	48
(一) 全面落實電子化作業制度: .....	48
(二) 建立系統預警機制: .....	48
(三) 增加使用查詢紀錄檔功能或延長保存時效: .....	48
(四) 落實職務輪調制: .....	49
(五) 建立系統需輸入申請人資料之機制: .....	49
(六) 權限之使用應配合個人自然人憑證: .....	49
(七) 辦理定期或不定期稽核作業: .....	49
二、執行面: .....	49
(一) 加強人員平時考核: .....	49
(二) 落實人員調動情形辦理帳號及權限異動: .....	50
(三) 加強落實機房之人員與物品管制: .....	50
(四) 對於硬碟或隨身碟報廢應落實以物理性破壞: .....	50
(五) 加強人員教育訓練: .....	50

(六) 加強資訊軟硬體設備：.....	51
捌、結語.....	51
附件：桃園縣政府 102 年使用個人資料查詢資訊系統專案稽核計畫.....	53

## 壹、前言

司法院大法官第 603 號解釋略以<sup>1</sup>：「個人資料之資訊隱私權，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權」。在此種思維下我國「資訊隱私權」（Information Privacy）的概念乃因應而生，其中心思想乃在於：個人不僅是個人資料產出的最初來源，也是其正確性、完整性的最後查核者，以及該個人資料的使用範圍的參與決定者。因此法務部極力推動「個人資料保護法」（下稱個資法）的修法，並於 101 年 10 月 1 日施行，相較於原有之「電腦處理個人資料保護法」，該法已擴大保護客體，不再以電腦處理之資料為限，人工蒐集、處理之個人資料亦適用之，公務機關及所有行業之企業、團體及個人等非公務機關均納入適用主體，影響範圍層面頗大。

為確保本府各機關人員使用個人資料相關查詢資訊系統具合法與正當性，防範個資外洩，本府前以 102 年 3 月 7 日府政安字 10200571025 號函請警察局、稅務局、衛生局、民政局、地政局等機關就使用個人資料資訊系統辦理專案稽核，俾維民眾隱私、財產等憲法上基本權利，落實資訊安全與公務機密之管理。

前揭專案稽核計畫由本處訂定，於 102 年 4 至 7 月稽核本府 52 個所屬機關(或單位)<sup>2</sup>使用個人資料資訊系統 47 個項目，稽核人數 482 人次<sup>3</sup>，稽核資料 1250 筆，期及早發掘個人資料外洩潛藏風險，另為使

<sup>1</sup>大法官釋字 603 號解釋文略以：維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障（本院釋字第五八五號解釋參照）。其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。惟憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第二十三條規定意旨之範圍內，以法律明確規定對之予以適當之限制。

<sup>2</sup> 本次專案稽核受稽核 52 個機關(單位)如次：(1)本府地方稅務局稽核總局各科室及中壢分局、大溪分局、楊梅分局。(2)衛生局稽核各鄉鎮市 13 個衛生所。(3)警察局稽核 10 個分局及 5 個大隊。(4)民政局稽核 13 個戶政事務所。(5)地政局稽核 7 個地政事務所。

<sup>3</sup> 本次專案稽核 482 人次，稽核機關正式及約聘僱人員統計至 6 月底止計 5499 人(資料來源：人事處)，稽核人數比例約為 8.77%。

本府各機關人員就個人資料保護法有深刻之瞭解，爰蒐羅相關學理學說、法令規定、資安維護措施、易滋弊端案例，併同前揭專案稽核發現之缺失態樣、建議事項等六大部分編撰本研析專報，俾供本府機關業務單位施政之參考。

## 貳、學說與學理之探討

### 一、個人資訊及隱私權的內容意涵：

所謂「隱私權」係指讓一個人不被打擾，安靜獨處生活的權利 (The Right To Be Let Alone)<sup>4</sup>；而「隱私」則指保護一個人在其不願意的情形下不被他人接近或接觸（無論是實際的身體接觸或是對個人資料的接觸，均包括在內）。如果由概念上進行分析，隱私權之概念，還可區分為消極意義與積極意義。前者強調個人私生活事務不受恣意公開干擾之權利；後者則是個人資料控制支配權，亦即賦予個人對其個人資料之蒐集利用發動權、停止權、內容提示權、更正權等；換言之，個人對於其個人資料應有主動積極控制支配之權利。如前所述，資訊隱私權屬於積極意義的隱私權，個人資訊的主體者享有相關權利，其具體內容茲分述如下<sup>5</sup>：

#### (一)個人資訊的取得、蒐集：

個人資訊的處理，與個人基本人權的保障具密切關係。縱使基於法律授權的「法律保留」<sup>6</sup>，也應受憲法上一定的約束，更何況非政府機關的商業蒐集。因此對於個人資

<sup>4</sup>1890 年美國聯邦大法官 Louis Brandies 對隱私權(Privacy)有一句名言闡釋--「The Right To Be Let Alone」，意即人民有安靜獨處的權利，所以「不被甘擾」應該就是隱私權的核心價值，區分為身體隱私權、通訊隱私權、領域隱私權、資訊隱私權。

<sup>5</sup> 參見林桓、余啓民、簡榮宗、葉奇鑫：政府機關強化個人資料保護措施之研究，頁 13-17，行政院研究考核發展委員會編印，2009 年。

<sup>6</sup> 法律保留原則又稱為積極的依法行政，謂沒有法律授權，行政機關即不能合法的作成行政行為，蓋憲法已將某些事項保留予立法機關，須由立法機關以法律加以規定，尤其以自由與財產(Freiheit und Eigentum)之侵害，嚴格限於須有法律之依據，參見吳庚「行政法之理論與實用」，頁 84、85，2000 年 9 月增訂六版。

訊的取得、蒐集，必須以適法、手段公正，且在達成目的之最小限度範圍內始得為之。而允許蒐集的個人資料範圍也應予以限制，例如思想、言論等與個人基本人權相關之資料，原則上禁止蒐集<sup>7</sup>。

## (二) 個人資訊的保有、管理、利用：

關於個人資訊的保有、管理、利用，基本上與前述資訊之蒐集相同，要兼顧「必要性」及「手段正當性」等憲法上之比例原則<sup>8</sup>。惟縱使資訊取得，蒐集手段正當，但若用於蒐集目的以外，仍構成隱私權之侵害。例如美國於 1974 年通過的隱私權法即規定，行政機關蒐集個人資訊後，除非有該法所列例外情形，否則其公開或移轉須經紀錄關係人之書面申請或同意。此種限制第二次利用的規定，正是此原則的實現<sup>9</sup>。

## (三) 個人資訊之閱覽、訂正請求權：

政府在積極給付行政<sup>10</sup>的運作之下，適時的介入國民生活，爰無法避免而被容忍，對國民也不得不提供個人資訊。惟隨腦科技的進步，個人的資訊隨時可能經由傳輸到達他人的手中，在此種情形下，若不賦予人民「確認個人資訊提供」之權利，則無異使個人置身於「無法確知自己是否成為被評價對象」的狀態之中。因此，人民對於自己

<sup>7</sup> 參見簡榮宗，網路上資訊隱私權保障問題之研究 (<http://www.cyberlawyer.com.tw/>)。

<sup>8</sup> 比例原則源自德國，理論上被視為憲法位階之法律原則，以法律保留作為限制憲法上基本權利之準則者(參照憲法第 23 條)，一般均以比例原則充當內在界限。廣義之比例原則包括：適當性原則：國家所採取者必須是有助於達成目的的措施，又稱「合目的性原則」。必要性原則：如果有多種措施均可達成目的，國家應採取對人民侵害最小者，又稱「侵害最小原則」或「最小侵害原則」。狹義比例原則：國家所採取的手段所造成人民基本權利的侵害和所欲達成之目的間應該有相當的平衡(兩者不能顯失均衡)，亦即不能為了達成很小的目的而使人民蒙受過大的損失，又稱「衡量性原則」。亦即，合法的手段和合法的目的之間存在的損害比例必須相當。參見吳庚「行政法之理論與實用」，頁 57、58，290 年 8 月。

<sup>9</sup> 見註 7。

<sup>10</sup> 給付行政(Leistungsverwaltung)指以增進國民生活為目的，為二次世界大戰以後福利國家或給付國家之新型行政。態樣包括供給行政、社會保障行政及助益行政。參見李惠宗「行政法要義」，頁 8-9，五南圖書出版股份有限公司，2005 年 10 月。

是否成為他人之評價對象，或評價之基礎是否正確等確認手段之閱覽權便十分重要。而且，基於評價個人資訊正確之要求，一但發現資訊不正確，個人當然亦享有要求訂正之權利<sup>11</sup>。

由上述對於「資訊隱私權」權利性的理解可知，「資訊取得、蒐集的限制」以及「資訊保有、管理、利用的規定」，係排除來自第三者干涉之權利，屬於自由權排他性的一部份。而「資訊閱覽」或「資訊訂正」，則係某種作為的請求，在權利的性質上屬於請求權的一種。因此，資訊隱私權如同傳統的隱私權，除排除干涉的自由權性質外，還兼有請求權的性質。

## 二、隱私權的分類：

### （一）國外法制：

如就類別而言，一八九〇年美國聯邦大法官 Louis Brandies 曾將隱私權區分為四類：身體隱私權、通訊隱私權、領域隱私權、資訊隱私權等 4 項類別，另自西元 1970 年代初始，由於大量資訊自動化設備問世進入企業，企業中的 IT 系統開始提供管理上的效能，藉由查詢資料提供即時且精確的資訊，使管理者掌握組織運作狀況，做出適當的決策，公、私部門所掌握的資料與處理、利用方法越見增加，民眾對於此種現象產生警覺，遂要求保護隱私<sup>12</sup>。

為保護個人資料，相較於以往之單純意涵，美國之隱私權已不再只是「獨處的權利」，已擴張至透過隱私

<sup>11</sup> 見註 7。

<sup>12</sup> 政府早已存有人民的資料，私部門也開始進行相同的行為，相對應於 George Orwell 的不朽名著 1984 中的「老大哥」（Big Brothers），學者創造出「小大哥」（Little Brothers）這個名詞描述公、私部門均進行個人資料蒐集的行為。

權保障的賦予，維護個人自主性（Personal Autonomy）與個人的身分認同（Personal Identity），以達到維護個人基本尊嚴（Personal Dignity）的目的<sup>13</sup>，換言之，隱私權已擴充為可「控制自身資訊的權利」；引申而來的「資訊隱私權」除了包含個人事務不受他人公開干擾的消極權利外，並包括在沒有通知當事人並獲得其同意之前，不得逕行蒐集當事人之個人資料，以及資料持有者不可將當事人為某特定目的所提供的資料用於其他目的。

## （二）司法院大法官解釋：

我國大法官會議就「隱私權」部分，曾做出以下解釋，以呼應社會各界對於保護個人隱私權上之需求，其類別區分為二：

### 1、隱私權：

隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障。（大法官會議釋字第 585 號解釋<sup>14</sup>）

<sup>13</sup> 劉靜怡，網際網路時代的資訊使用與隱私權保護規範：個人、政府與市場的拔河，資訊管理研究，第四卷，頁 144-145，2002 年。

<sup>14</sup> 大法官釋字 585 號解釋部分理由略以：國家機關行使權力均須受法之節制，立法院行使憲法所賦予之權力，亦無例外，此乃法治原則之基本要求。立法院調查權之行使，依調查事項及強制方式之不同，可能分別涉及限制多種受憲法保障之人民基本權利，如憲法第八條保障之人身自由、憲法第十一條保障之消極不表意自由（本院釋字第五七七號解釋參照）、憲法第十二條保障之秘密通訊之自由、憲法第十五條所保障之營業秘密、隱私權……等等。其中隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障（司法院釋字第五〇九號、第五三五號解釋參照）。

## 2、資訊隱私權：

就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。（大法官會議釋字第 603 號解釋<sup>15</sup>）

綜合釋字第 585 號解釋及 603 號解釋可知，在層級上，隱私權為資訊隱私權之上位概念；資訊隱私權則係個人資料之上位概念。

### 參、現行法令規範及本府各機關行政程序：

#### 一、個資法立法沿革：

以往「電腦處理個人資料保護法」自 84 年 8 月 11 日公布施行近 18 年，由於資訊通信科技發達的結果，透過電腦及網際網路處理與傳輸個人資料之情形已今非昔比，該法規範顯有不足，且個人資料外洩事件時有所聞，尤其是尚有龐大未適用該法的民間產業，影響民眾個人資料之隱私權益甚鉅。有鑑於此，法務部遂組成修法專案小組，並於 93 年間完成修正草案，歷經數年審議，於 99 年 4 月 27 日完成三讀，同年 5 月 26 日總統公布「個人資料保護法」，除第 6 條、第 54 條外，其餘條文行政院指定於 101 年 10 月 1 日施行。

<sup>15</sup>參見註 1。

表 1：個人資料保護法立法沿革一覽表

年度	立法情形
1993 年	行政院研擬完成「電腦處理個人資料保護法」草案，並送請立法院審議。
1995 年	立法院三讀通過「電腦處理個人資料保護法」草案，同年總統公布施行。
2005 年	法務部研擬完成「電腦處理個人資料保護法」草案，並將法規名稱改為「個人資料保護法」，並送請立法院審議。
2010 年	4 月 27 日立法院三讀通過個人資料保護法，總統府並於 5 月 26 日正式公告新法（101 年 10 月 1 日施行）。

## 二、個資法新法修正重點：

有關此次個資法之修正重點，茲分述如下<sup>16</sup>：

### (一)擴大保護客體及名稱之修正：

落實對個人資料之保護，將保護客體予以擴大，不再以經電腦處理之個人資料為限，人工蒐集、處理之個人資料，亦適用之（新法第 2 條第 2 款及第 4 款），爰將該法名稱修正為「個人資料保護法」。在個人資料的定義部分，新法將所謂之「個人資料」予以明確化，包含自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。（新法第 2 條第 1 款）另個人資料中有部分資料性質較為特殊或具敏感性，如任意蒐集、處

<sup>16</sup> 詳見法務部網站「個人資料保護法專區」（<http://pipa.moj.gov.tw>）

理或利用，恐造成社會不安或對當事人造成難以彌補之傷害，故另規定較嚴格之蒐集、處理或利用要件。該特種資料包括醫療、基因、性生活、健康檢查及犯罪前科之 5 種個人資料屬特種資料。

**表 2：個人資料保護法一般資料與特種資料對照表**

一般資料	特種資料
生存自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、聯絡方式、財務情況、社會活動	醫療、基因、性生活、健康檢查、犯罪前科

**(二) 擴大適用主體及領域：**

本次修法刪除非公務機關行業別之限制，使任何自然人、法人或其他團體，原則皆須適用新法。（新法第 2 條第 8 款）另公務機關及非公務機關，在中華民國領域外對中華民國人民蒐集、處理或利用個人資料者，亦有新法之適用。（新法第 50 條第 2 項）<sup>17</sup>

**(三) 不定義主管機關：**

法務部僅是該法解釋機關，在不設置中央及地方專責機關前提下，直接於各條文中明定由中央目的事業主管機關或直轄市、縣（市）政府共同辦理。

<sup>17</sup>簡言之，個資法裡將適用對象區分成兩類：公務機關及非公務機關。舊法裡非公務機關包含了下列八大行業：徵信業以及搜集或電腦處理個人資料為主要業務之團體或個人、醫院、學校、電信業、金融業、證券業、保險業、大眾傳播業，及其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。新修正的個資法則將非公務機關定為公務機關以外的自然人、法人或其他團體，有別於舊法所指定的行業，將適用對象擴及至公民營機關及個人。

(四)新法排除適用範圍：

修法後明定有下列情形之一者，不適用新法規定：

- (一) 自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。(新法第 50 條第 1 項第 1 款)
- (二) 於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。(新法第 50 條第 1 項第 2 款)

(五)特種個人資料之蒐集、處理或利用：

有關醫療、基因、性生活、健康檢查及犯罪前科等五類資料為特種資料，除符合法定要件外<sup>18</sup>，原則上不得蒐集、處理或利用。(新法第 6 條)

表 3：個資法所述行為態樣情形一覽表

蒐集：指為建立個人資料檔案而取得個人資料指以任何方式取得個人資料，包含直接向當事人蒐集者，以及間接從第三人取得者。
處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
利用：指將蒐集之個人資料為處理以外之使用。
國際傳輸：指將個人資料作跨國(境)之處理或利用包含機關內部之資料傳送(資料處理)，以及將資料提供當事人以外之第三人(資料利用)。

(六)蒐集、處理或利用資料前之告知義務：

<sup>18</sup>例外情形：1、法律明文規定。2、公務機關依法或非公務機關履行法定義務所必要。3、當事人自行公開或其他已合法公開者。4、公務機關或學術研究機構基於醫療衛生或犯罪預防目的。

不論是直接或間接蒐集資料，除符合得免告知情形者外，均須明確告知當事人蒐集機關名稱、蒐集目的、資料類別、利用方式、資料來源等相關事項。另為減少勞費起見，允許得於首次對當事人為利用時得併同告知（新法第8條及第9條）。若新法修正施行前非由當事人提供之個人資料，依第9條規定應於處理或利用前向當事人為告知者，應自新法修正施行之日起1年內完成告知，逾期未告知而處理或利用者，以違反第9條規定論處（新法第54條）。

（七）增強個人資料當事人之權利：

為保障人民自主控制個人資料之資訊隱私權，當事人得就其個人資料行使請求查詢、閱覽、製給複製本、補充或更正、停止蒐集、處理或利用、刪除等權利（新法第3條），惟於妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益、妨害公務機關執行法定職務、妨害該蒐集機關或第三人之重大利益等情形例外排除當事人上開之權利（新法第10條）。

違反新法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除或停止蒐集、處理或利用其個人資料；公務機關和非公務機關對其所保有之個人資料，並有更正、補充及通知之義務（新法第11條）。

非公務機關於利用個人資料從事商品行銷時，不論係目的內或目的外利用，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷，並且於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。（新法第20條第2項、第3項）。

(八) 明定一般資料之蒐集、處理及利用要件：

1、公務機關蒐集、處理個人資料之要件(新法第 15 條)：

- (1) 執行法定職務必要範圍內。
- (2) 經當事人書面同意。
- (3) 對當事人權益無侵害。

2、公務機關利用個人資料之要件(新法第 16 條)：

公務機關對個人資料之利用，除第 6 條第 1 項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的之外之利用：

- (1) 法律明文規定。
- (2) 為維護國家安全或增進公共利益。
- (3) 為免除當事人之生命、身體、自由或財產上之危險。
- (4) 為防止他人權益之重大危害。
- (5) 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。
- (6) 有利於當事人權益。
- (7) 經當事人書面同意。

3、非公務機關之蒐集、處理個人資料之要件(新法 19 條)：

- (1) 法律明文規定。
- (2) 與當事人有契約或類似契約之關係。
- (3) 當事人自行公開或其他已合法公開之個人資料。
- (4) 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。

- (5) 經當事人書面同意。
- (6) 與公共利益有關。
- (7) 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

4、非公務機關利用個人資料之要件(新法第 20 條)：

- (1) 法律明文規定。
- (2) 為增進公共利益。
- (3) 為免除當事人之生命、身體、自由或財產上之危險。
- (4) 為防止他人權益之重大危害。
- (5) 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。
- (6) 經當事人書面同意。

表 4：公務機關與非公務機關於特定目的內蒐集、處理個人資料要件一覽表

公務機關	非公務機關
法定職務必要範圍	法律明文規定
當事人書面同意	有契約或類似契約關係
對當事人權益無侵害	自行公開或其他已合法公開者
	學術研究機構基於公共利益為統計或學術研究之必要，且處理後或揭露時無從識別特定當事人
	當事人書面同意
	與公共利益有關

	取自一般可得之來源，但有更值得保護之利益者除外
--	-------------------------

**表 5：公務機關與非公務機關於特定目的外利用個人資料要件一覽表**

公務機關	非公務機關
法律明文規定	
維護國家安全或增進公共利益	為增進公共利益
免除當事人之生命、身體、自由或財產上危險	
防止他人權益之重大危害	
公務機關或學術研究機構基於公益為統計或學術研究之必要，且資料經處理後或依其揭露方式無從識別特定之當事人	
有利於當事人權益	
經當事人書面同意	經當事人書面同意

(九) 明定書面同意之定義：

新法所稱書面同意，指經蒐集者告知新法所定應告知事項後，所為允許之書面意思表示。特定目的外利用個人資料需當事人書面同意者，不得以概括方式取得其同意，而應另以單獨書面同意方式為之，以確保當事人之權益。（新法第 7 條）

(十) 強化行政監督：

1、主管機關之檢查措施(新法第22條)：

為加強防制個人資料之濫用，中央目的事業主管機關或直轄市、縣（市）政府，發現非公務機關違反新法規定或認

有必要時，得派員攜帶執行職務證明文件，進入檢查，如發現有違法情事，並得採取必要處分。

2、當事人不服檢查措施之救濟方法(新法第 24 條)

中央目的事業主管機關或直轄市、縣(市)政府執行檢查時所採取之措施，或相關強制、扣留或複製行為，當事人如有不服，得聲明異議。

3、違反新法規定之必要處分(新法第 25 條)

中央目的事業主管機關或直轄市、縣(市)政府，發現非公務機關蒐集、處理或利用個人資料有違反新法規定之情形者，除依法裁處罰鍰外，得採取禁止蒐集、處理或利用個人資料、命令刪除、予以沒入或命銷毀違法蒐集或處理之個人資料、公布姓名等必要處分，以保護資料當事人之權益不被繼續侵害。

(十一) 團體訴訟：

1、為結合民間力量，發揮新法保護個人資料之功能，爰增訂財團法人或公益社團法人符合新法規定者，得提起團體訴訟，以協助遭侵害之當事人進行損害賠償訴訟。(新法第 32 條)

2、為鼓勵當事人透過團體訴訟主張權利，增訂團體訴訟裁判費減免之規定。(新法第 33 條)

(十二) 相關責任：

1、刑事責任：

對於違法蒐集、處理或利用個人資料者，區別其是否具有「意圖營利」之主觀要件，科予程度不等之刑事責任。

- (1)無營利意圖者(新法第 41 條第 1 項)可處以二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。
- (2)意圖營利者(新法第 41 條第 2 項、第 42 條)可處以五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。另如意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，可處以五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。為提升法益保護之周延程度，中華民國人民在我國領域外觸犯新法之罪者，亦適用新法(新法第 43 條)。

## 2、調整損害賠償責任限制額度：

### (1)每人每一事件賠償額度降低

被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，從每人每一事件新臺幣2萬元以上10萬元以下，改為以新臺幣500元以上2萬元以下計算(新法第28條第3項)。

### (2)同一原因事實賠償總額提高

提高基於同一原因事實應對當事人負損害賠償責任之總額，由新臺幣2千萬元提高至新臺幣2億元(新法第28條第4項)。

## 3、行政罰責任

非公務機關如違反新法規定，依其違法行為態樣得課以不同程度之行政罰責任：

- (1) 違法蒐集、處理或利用特種個資或一般資料，或違反中央目的事業主管機關依新法第21條規定所為限制國際傳輸之命令或處分者，處新臺幣5萬元以上50萬元以下罰鍰(新法第47條)。
- (2) 違反新法有關告知義務，當事人之相關權利，個人資料被竊取、洩漏、竄改或其他侵害之通知義務，或行銷應給予拒絕接受行銷之方式規定，先限期改正，屆期未改正者，按次處新臺幣2萬元以上20萬元以下罰鍰(新法第48條)。
- (3) 非公務機關無正當理由規避、妨礙或拒絕目的事業主管機關進入、檢查或處分者，處新臺幣2萬元以上20萬元以下罰鍰(新法第49條)。
- (4) 非公務機關之代表人、管理人或其他有代表權人，因該非公務機關違反新法規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰(新法第50條)。

### 三、本府各機關相關法令規定與行政流程：

#### (一) 警察局：

##### 1、法令依據：

- (1) 行政院及所屬各機關資訊安全管理要點。
- (2) 警察機關公務機密維護實施規定。
- (3) 警察機關資訊安全實施規定。
- (4) 警用行動電腦使用管理要點。
- (5) 內政部警政署資訊系統使用者帳號及權限管理規定。
- (6) 內政部警政署戶役政資訊電子閘門系統作業管理規

定。

(7)內政部警政署受理刑案資料查詢作業規定。

(8)內政部警政署車籍資訊系統查詢作業規定。

## 2、行政流程:

(1) 警政知識聯網查詢作業密碼由內政部警政署配發各使用單位，經各使用單位配賦各終端工作站相關人員查詢作業時使用。

(2) 各項系統均由內政部警政署資訊室負責該系統資料維護、代碼維護、系統維運、轉檔監控及異常資料處理等工作。

(3) 各項系統承辦人（管理者）使用權限設定、審核及督導工作，該系統權責管轄權，則由內政部警政署業務（科）組負責。

(4) 各項系統使用者權限設定、審核及督導工作，則由直轄市、縣（市）警察局及專業警察機關資訊單位負責。

### (二) 其他機關就戶役政資訊系統部分:

#### (一) 法令依據:

(1) 行政院及所屬各機關資訊安全管理要點。

(2) 桃園縣政府縣政資料庫查詢系統作業要點。

(3) 連結戶役政資訊系統本府各需求機關部分:

甲、地方稅務局：依據財政部之「稅務機關使用戶役政資訊管理規定」。

乙、衛生局：「行政院衛生署使用戶役政資訊連結作業管理規範」。

丙、地政局：依據內政部之「地政業務應用戶役政資訊系統查詢戶籍資料作業管理規定」之授權，研

訂「桃園縣政府地政局應用戶役政資訊系統查詢戶籍資料作業管理規定」。

丁、民政局：桃園縣政府戶役政資訊系統電腦作業準則。

## 2、作業流程：

### (1) 申請使用者通行碼：

因業務需要須使用戶籍資料者，應依程序申請使用通行碼(含帳號及密碼)，並填寫「使用戶役政資訊系統帳號異動申請單」。各機關申請使用之帳號由資訊單位管理其查詢帳號開立、權限審核。

### (2) 限使用人本人使用帳號查詢資料：

非經配用通行碼之人員，不得擅自利用他人之通行碼查詢資料。通行碼使用人僅得為公務之需要查詢資料，不得為公務以外之利用。查詢資料及相關使用規範，應符合個人資料保護法之規定。

### (3) 設立專人管理之查詢戶籍資料登記簿：

承辦人員查詢時將文號或案號及一項被查詢人資料(如姓名、國民身份證統一編號、相關名稱等可供事後稽核者)為代表，詳實登記於登記簿上，該登記簿一律陳送單位主管或其授權人核閱後備查。

### (4) 建立查詢通行碼管理制度：

由專人負責管理，並指定職務代理人，查詢通行碼之管理者職務有異動時，應將所負責保管之相關文件資料列冊移交。接辦人員應另行申請更改密碼，以利管理。

### (5) 使用者異動：

經配用通行碼之使用者其職務有異動時，管理者即取消其使用權，其職務接辦人員應重新申請通行碼。

#### 肆、本國與外國有關個人資料與資訊安全之維護措施：

個資法施行細則第 12 條對於公務機關個資保護的要求，即「適當安全維護措施(第 6 條第 1 項第 2 款)」、「安全維護事項(第 18 條)」等，係指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。以下即就本國與外國有關個人資料與資訊安全之維護措施予以探討：

##### 一、我國有關個資資訊安全之維護措施：

從 2003 年起，我國累積了數百組織取得符合 ISO27001 國際資訊安全管理系統驗證標準之證書，放眼全球，台灣在資訊安全證書取得的量上，已與其他先進國家不遑多讓；儘管個人資料的保護雖與資訊安全控管有許多重疊之處，但台灣在資訊安全管理系統推動上，多著眼於資訊部門的管理，對於推動涵蓋範圍是否已適當，而不至於會有「雖取得證書，但仍發生於驗證範圍外之資料外洩事故」情形發生，實有太多不可臆測之因素。

##### 二、外國有關個資資訊安全之維護措施：

###### (一) 歐美國家部分：

由於歐美等國對於個資保護十分重視，個資法施行細則的立法說明亦明揭相關規定是參照英國 BS10012:2009<sup>19</sup> 及日本 JISQ15001:2006 等個人資料管理系統的規範。因此，雖然國情未必相同，公務機關應如何建立個資保護環

<sup>19</sup> 此為 BSI 英國標準協會在 2009 年發佈的個人資料管理系統 (Personal Information Management System, PIMS)，轉引自鍾文岳、汪家倩著，〈個人資料保護法，這樣讀就對了—企業篇〉，《萬國法律》，181 期，民國 101 年 2 月，頁 13。

境，上開國家在個資管理的實務經驗頗值參考。學者參考 BS10012：2009 規範與我國個資法施行細則對於個資保護環境的 11 項要求，對個資保護環境的建立、檢討及改善等，提供以下建議<sup>20</sup>：

	個資法施行細則第 12 條規定	參考英國 BS10012：2009 後的建議
1	成立管理組織，配置相當資源	建立公司個資管理的政策 成立管理組織(例如資訊管理部門)，適當界定、分配角色與職責 對個資的管理及保護進行規劃、管理 對個資保護的資源進行規劃、管理 定期檢討進度與改善
2	界定個人資料之範圍	依新個資法界定並區分一般個資及特種個資 考量不同類型個資應適用的法律、規定、合約條款等 考量不同個資的性質及範圍，以決定保護策略
3	個人資料之風險評估及管理機制	評估個人資料可辨識的容易程度、個資數量、敏感程度、用途等，建立評估個資保護及相關個人風險程度的流程 依前開評估，妥善管理已知或可得而知的風險，並建立陳報及審查的程序
4	事故之預防、通報及應變機制	建立個資事故的標準作業程序，例如如何預防或減緩損害、如何紀錄個資事故、如何通報或通知(公司內部、主管機關、當事人)、如何應變等

<sup>20</sup> 鍾文岳、汪家倩著，前揭文，頁 14-15。

		<p>就各項個資事故的發生及處理，留下完整紀錄，以便查知處理情形、並可用於檢討及改進個資保護環境之用</p>
5	<p>個人資料蒐集、處理及利用之內部管理程序</p>	<p>就公司的個資保護政策及上述資源配置、風險評估及管理、預防、通報、應變機制等，依公司之行業別及業務屬性，建立適當的內部標準作業程序</p> <p>將內部管理程序以適當方式公告、告知相關人員</p>
6	<p>資料安全管理及人員管理</p>	<p>採行適當的技術及安全措施，以確保個資受到保護，不致遺失、或遭未經授權的利用等</p> <p>至少包括安全控制措施、儲存與處理的機制、傳輸、存取控制、安全評估等機制</p> <p>上述措施，不應低於該時期一般可採行的技術水準，例如不應低於同業普遍採取的安全管理措施程度等</p>
7	<p>認知宣導及教育訓練</p>	<p>於適當時期進行宣導及教育訓練，促使相關人員在接觸個人資料時切實明白自身的角色、職責、應遵循的法規、公司作業規範等，例如在新進人員的員工訓練加入相關說明、定期舉辦教育訓練或考核等</p>
8	<p>設備安全管理</p>	<p>指定專人負責管理處理及儲存個資的設備，例如電腦主機及周邊設備等</p> <p>加強防護天然災害、意外及其他外部入侵的預防及應變措施</p> <p>相關設備的維修、更新、報廢時，指派專人處理，以防止個資外洩，設備廢棄或不使用時，應確實</p>

		刪除個人資料檔案，包括其備份檔案及軌跡資料（例如 Log Files、網路位址等）
9	資料安全稽核機制	建立個資檔案稽核制度，包括內部稽核程序等 指定專人定期或不定期稽核個資使用情形 處理個人資料時，核對該資料之編輯、輸入等情形是否與原檔案或更新後之事實相符
10	必要之使用紀錄、軌跡資料及證據之保存	建立內部制度，適當決定各類個人資料保存的環境、條件、期限等 紀錄個人資料檔案的使用情形、存取者、時間、設備、用途等，並保留相關電子或書面資料以供日後存取查閱
11	個人資料安全維護之整體持續改善	針對已採取的個資保護政策及程序、每一不同時期可得採取的個資保護措施、相關資安等技術水準定期檢討 針對曾發生的個資事故加以檢討、提出防止事故發生之對策 提出公司個資保護環境長期改善計畫，並予執行
註	以上的必要措施，以所需支出之費用與所欲達成個人資料保護目的符合適當比例者為限	

(二) 日本部分：

日本在 2003 年通過相當於我國個資法之「個人情報保護法」後，財團法人日本情報處理開發協會（JIPDEC）便以此為基礎，建立結合法制與管理制度的「JISQ15001：2006」。個資法及其施行細則中所謂「採取適當安全維護措施」該如何解釋，端視我國未來所建置個人資料保護管

理制度內容而定，目前仍有待觀察，故現階段 JIPDEC 以 JISQ15001：2006 為基礎所作成的處理原則中，對於安全管理措施所提出的檢查項目（詳參下表），於個資法施行細則所要求的 11 大項內容之解釋適用仍十分具有參考價值<sup>21</sup>。

安全管理措施	檢查項目
1. 物理的安全管理措施	
1.1 進出館(室)管理	<p>有限制進出建築物、房間、機房、個人情報處理場所之機構。</p> <p>限制進出建築物、房間、機房、個人情報處理場所。做成、保管進出建築物、房間、機房、個人情報處理場所之紀錄。</p> <p>定期確認進出建築物、房間、機房、個人情報處理場所之紀錄。</p>
1.2 竊盜等之防止	<p>離開座位時不將記載個人資料之文件媒介物、攜帶型電腦放置於桌上。</p> <p>操作處理個人資料之電腦，於離開座位時應啟動設有密碼之螢幕保護裝置或登出。</p> <p>將記載個人資料之媒介物（紀錄媒介物、紙張）上鎖保管，掌握應有的東西皆俱全。</p> <p>記載個人資料之媒介物（紀錄媒介物、紙張）之保管場所的鑰匙由特定人管理。</p> <p>實施不得再利用已作廢丟棄之記載個人資料之媒介</p>

<sup>21</sup> 參照鍾文岳、鄭雯婷著：〈公務機關適用個人資料保護法之今後方向與課題—以日本實務經驗為借鏡〉，《萬國法律》，181期，民國101年2月，頁25、頁27-29。

	<p>物（紀錄媒介物、紙張）之相關措施。</p> <p>對有紀錄個人資料之攜帶型電腦等設置防盜措施。</p> <p>遵循 FD、MD、CD、USB 隨身碟等外部記憶體的利用規則。</p> <p>不將個人資料處理資訊系統的操作手冊置於桌上。</p>
1.3 機器・裝置等的 物理保護	<p>對處理個人資料之機器・裝置等，設有防止安全管理上威脅（竊盜、破壞、毀損等）及環境上威脅（漏水、火災、停電、地震等）之物理性保護裝置。</p>
2. 技術的安全管理措施	
2.1 接觸（access） 個人資料時之 識別與認證	<p>就個人資料之接觸，實施識別資訊（ID、密碼等）之認證。</p> <p>含有個人資料在內的資訊系統不留預設值之設定。</p> <p>識別資訊之發行、更新、廢棄遵循規定。</p> <p>識別資訊不以未暗號化（按：「暗號化」指轉變為不易解讀的暗號）之方式紀錄。</p> <p>設定密碼有效期限、限制再次使用同一或類似密碼、設定最低密碼字數、將一定次數登入失敗的 ID 停權等措施。</p> <p>以 MAC 位址認證、IP 位址認證、使用電子證明書和秘密分散技術之認證等措施對具有接觸個人資料權限之業者得使用之終端或位址等加以設限。</p>
2.2 接觸個人資料 時之管制	<p>限制得接觸個人資料之業者數量於必要最小範圍。</p> <p>不由多數人共用可接觸個人資料之識別資訊。</p> <p>於必要最小範圍內賦予業者接觸權限。</p> <p>限制含有個人資料在內的資訊系統於同一時間內之利用人數。</p>

	<p>限制含有個人資料在內的資訊系統的利用時間。</p> <p>保護含有個人資料在內的資訊系統不受無權限接觸。</p> <p>防止無權限使用可能會去接觸到個人資料之應用軟體。</p> <p>查驗對個人資料處理資訊系統所導入之接觸控制機能的有效性。</p>
<p>2.3 接觸個人資料 權限之管理</p>	<p>適切且定期實施許可得接觸個人資料者之管理權限。</p> <p>將對個人資料處理資訊系統之接觸控制在必要最小範圍內。</p>
<p>2.4 接觸個人資料 之紀錄</p>	<p>取得、保管接觸個人資料與操作成敗之紀錄。</p> <p>對取得之紀錄給予適切保護，避免洩漏、滅失及毀損。</p>
<p>2.5 關於個人資料 處理資訊系統 之不正軟體對 策</p>	<p>導入防毒軟體，並經常更新至最新版本。</p> <p>對 OS 和應用軟體等適用系統安全性更新 (security patch)。</p> <p>確認不正軟體對策之有效性、安定性。</p> <p>不在可接觸個人資訊之終端安裝檔案分享軟體 (Winny 和 Share 等 P2P 分享軟體)</p>
<p>2.6 個人資料的移 送・通信時的對 策</p>	<p>保留個人資料之收發紀錄。</p> <p>擬定以媒介物移送個人資料時，移送時遺失・竊盜發生時的對策。</p> <p>以可能遭竊聽的網路(例如：網際網路和無線 LAN 等)傳送(例如包含以本人及業者輸入和接觸，以 mail 附加檔案等方式傳送檔案等)個人資料時，將個人資料暗號化(按：轉變為不易解讀的暗號)或以密碼上鎖等。</p>

2.7 個人資料處理 資訊系統之動 作確認時之對 策	不以個人資料作為確認資訊系統動作時的測試資料。 查證變更資訊系統時，該變更不會造成資訊系統或運 用環境安全的損害。
2.8 個人資料處理 資訊系統之動 作確認時之監 視	定期檢查個人資料處理資訊系統的使用狀況。 定期檢查接觸個人資訊之狀況（含操作內容）。

## 伍、可能易滋弊端態樣研析

### 一、公務部門案例類型：

#### (一) 查詢他人個資供己使用：

##### 1、案例情節

甲於民國 96、97 年間，係任職於財政部某區國稅局（下稱某區國稅局）稅務員之職務，為公務員。其明知納稅義務人提供之財產、所得、營業及納稅等資料，係關於中華民國國防以外應秘密之資料以及他人之秘密，非依法令規定不得無故對外洩漏或交付因利用電腦知悉或持有之前開資料，及在其公務範疇內始得進入稅務系統查詢他人資料，竟基於公務員洩漏國防以外秘密，以及洩漏利用電腦知悉他人之秘密之犯意，於 97 年 1 月 15 日利用職務上得調閱某區國稅局稅務系統資料權限之機會，在某區國稅局辦公室內，以電腦進入稅務系統查詢乙之各類所得扣繳暨免扣繳憑單資料（下稱系爭資料），並

將該資料加以列印，嗣於翌日在其與乙間誹謗案件之公開審理庭中(96年度簡上第636號案件，下稱系爭案件)，將系爭資料提出作為證據而交付此國防以外應秘密之文書予他人，以供其私人訴訟之用，後遭人舉發在案。

## 2、所涉及之法律責任

(1) 按刑法第 132 條第 1 項規定略以，公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。（洩漏國防以外之秘密罪）另刑法第 318 條之 1 規定略以，無故洩漏因利用電腦或其他相關設備知悉或持有他人之秘密者，處 2 年以下有期徒刑、拘役或 5 千元以下罰金。

(2) 甲擔任稅務員職務，卻利用職權機會查詢應予保密之個人資料，顯已違反前揭法令，經衡諸案情，臺灣○○地方法院 99 年 4 月 16 日 99 年度易字第 349 號判決主文略以：甲犯公務員洩漏、交付國防以外之秘密文書罪，處有期徒刑肆月，得易科罰金，以新臺幣壹仟元折算壹日<sup>22</sup>。

## (二) 接受朋友請託代為查詢：

### 1、案例情節

(1) 甲係○○市警察局警員，於 96 年 9 月 17 日因受民眾陶○○電話請託，藉其職務關係先以電腦檢索方式探知陶○○之債務人「胡○○」個人資料，再於同年 9 月 19、20 日左右，逕往陶○○住居所○○市光華國宅，將「胡○○」之個人資料面告陶○○，藉

<sup>22</sup> 見臺灣高雄地方法院 99 年 4 月 16 日 99 年度易字第 349 號判決。

此而對當事人以外之第三人洩漏關於中華民國國防以外應秘密之消息，案經法務部調查局臺北市調查處移送臺灣○○地方法院檢察署偵辦。案經偵查終結，並經檢察官提起公诉，臺灣○○地方法院 99 年度基簡字第 18 號刑事簡易判決略以：「甲○○公務員洩漏關於中華民國國防以外應秘密之消息，處有期徒刑肆月，得易科罰金，以新臺幣壹仟元折算壹日。」<sup>23</sup>

(2) 甲○○前於○○縣警察局刑事警察大隊配置○○分局偵查隊偵查佐職務期間，明知一般民眾之個人戶籍資料或涉個人隱私或攸關國家之政務或事務，均屬國防以外應秘密之資料，公務員負有保守秘密之義務，竟基於公務員洩漏國防以外秘密之犯意，於民國 93 年 3 月 11 日下午 5 時 27 分許，因其經營酒店之友人王○○以電話請託甲○○查詢民眾林○○之行蹤資料，甲○○竟接受其委託，於同日下午 6 時 29 分，私下以其服務單位分隊長之帳號、密碼進入警政署資訊室戶役政資訊電子閘門查詢之戶役政資料後，隨即於同(11)日 18 時 33 分致電王○○，並告知其查詢之林○○戶籍所在位置及相關戶口資料等訊息<sup>24</sup>。

(3) 陳○○係○○縣政府行政室○○，自 78 年間進入○○縣政府服務迄今，職司○○縣政府所轄各機關公文封發、付郵及郵資結算業務，係依據法令從事公務之人員。91 年 7 月至 93 年 3 月間，陳○○明

<sup>23</sup> 見臺灣基隆地方法院 99 年度基簡字第 18 號刑事簡易判決。

<sup>24</sup> 見臺灣高雄地方法院 98 年度審易字第 1688 號刑事判決。

知○○縣各醫療院所通報○○縣政府衛生局之新生兒出生證明書，為該府業務上應秘密之文書，不得無故洩漏或交付予他人，竟於前述期間，基於概括犯意，由陳○○利用○○縣政府行政室收到轄內各醫療院所通報該府民政局新生兒出生證明書之機會，將職務上所持有之新生兒出生證明書，篩選出王○○指定之二至三家醫療院所通報之新生兒出生證明書，影印郵寄影本予王○○，每月寄送一次，共寄送 21 次，每次寄送五至七張，累計陳○○於前述期間共洩漏產婦及新生兒資料達 105 筆以上。案經檢察官偵查以陳員觸犯刑法第 132 條第 1 項「公務員洩漏或交付關於中華民國國防以外秘密」罪嫌提起公诉，臺北地方法院經審理後，判處陳員有期徒刑 3 月，得易科罰金，以銀元 300 元即新台幣 900 元折算 1 日，緩刑 2 年<sup>25</sup>。

## 2、所涉及之法律責任

- (1) 按刑法第 132 條第 1 項規定略以，公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處 3 年以下有期徒刑。（洩漏國防以外之秘密罪）
- (2) 文中承辦人等將查詢資料洩漏予友人，雖基於私人之情誼，亦已觸犯相關法條，上開案例足堪身為公務員者警惕。

<sup>25</sup>見臺灣台北地方法院 93 年度訴字第 1157 號判決。

### (三) 協助他人營利：

#### 1、案例情節

某公司業務人員陳○○曾從事護理工作，瞭解嬰兒奶粉、彌月蛋糕、油飯等廠商亟需產婦及新生兒個人資料作為寄送型錄及試用品之用，乃藉由過去從事護理工作之人脈，認識縣市衛生局負責或能接觸產婦及新生兒個人資料之公務員林○○，以公司業務需要為由，希望林○○越權查詢出生通報系統等方法提供產婦及新生兒個人資料，再由其公司員工將資料上所列產婦及新生兒等個人資料輸入電腦建檔處理，以利將資料販售給食品公司等家廠商<sup>26</sup>。

#### 2、所涉及之法律責任

(1) 按刑法第 132 條第 1 項規定略以，公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處 3 年以下有期徒刑。（洩漏國防以外之秘密罪）

(2) 林○○因欠缺保密觀念，遂協助陳○○調閱資料，致其成為陳○○取得產婦及新生兒個人資料之捷徑，不但該公司侵害各產婦及新生兒之隱私權而觸法；且林○○亦因而涉及刑法第 132 條第 1 項洩漏國防以外之秘密罪嫌。

---

<sup>26</sup>同註 13。

(四) 收售價金與業者合謀：

1、 案例情節

- (1) 甲開徵信社，為順利取得客戶所需之入出境紀錄、地址、前科、通緝、更名與勞工保險等資料，乃與警員乙、丙聯絡，請乙代查上述相關資料，並依取得難易程度，每件以新台幣400至800不等之價額付予乙，先後甲總計共支付乙25萬6,702元。另請丙代查勞工保險資料，以每件200至1,500元不等之價額，甲共支付丙8萬3,400元。甲嗣後遭人檢舉，經檢調單位偵查屬實移送法辦，台灣高等法院依貪污治罪條例第4條第1項第5款「違背職務之行為，收受賄賂罪」，判處乙有期徒刑5年10個月，褫奪公權4年、丙有期徒刑5年4個月，褫奪公權3年，二人不法所得追繳沒收，如全部或一部分無法追繳時以其財產抵償之。另依同罪條例行賄罪，判處甲有期徒刑2年2個月，褫奪公權1年8個月<sup>27</sup>。
- (2) 另馬○○係某少年監獄會計室主任，其妻應○○則為某縣稅捐稽徵處電子登錄作業員，負責地價稅案件之登錄，操作電腦終端機調取資料非其主管事或監督之事務，自82年底起(馬○○自83年8、9月間開始)至84年2月間止，連續由三○徵信社負責人劉○○通知(原以電話或紙條方式，83年8、9月間改以傳真方式)，以身分證字號代查某縣之個人財產資料，同時應允每件給予400元(原為200元，後改為400

<sup>27</sup>見臺灣高等法院98年度重上更(五)字第137號刑事判決。

元)之報酬，並於 83 年 8、9 月間交付傳真機壹部，以為傳遞資料之用，應○○乃連續利用其在稅捐處得以接觸並操作電腦終端機之機會，將某縣稅捐處建檔儲存於電腦中應予保密之國防以外之機密個人財產資料叫出、抄寫後，83 年 8、9 月以前由劉○○親自至某縣稅捐稽徵處附近天橋下拿取資料，83 年 8、9 月後即由應○○或由馬○○在其等住處以傳真機將查詢資料以傳真方式交給劉○○，而洩漏中華民國國防以外應秘密之文書，迄被查獲為止，共圖得 20 萬元之不法利益。案經檢察官偵查後提起公訴，地方法院判處馬○○有期徒刑伍年，褫奪公權貳年；其妻應○○有期徒刑貳年陸個月，褫奪公權貳年。所得財物新台幣貳拾萬元，追繳沒收之<sup>28</sup>。

## 2、所涉及之法律責任

- (1)按刑法第 132 條第 1 項與第 2 項規定略以：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處 3 年以下有期徒刑。因過失犯前項之罪者，處 1 年以下有期徒刑、拘役或 300 元以下罰金。」。
- (2)戶政單位或其他類如警察、稅捐、電信等機關人員係依據業務職掌經營公務機密資料，理應恪遵作業規定，予以保密，不得洩漏於外，即或在人情困擾下，亦不得破例，否則民眾權益及個人隱私勢將受損，坊間多有徵信業者從事錄音、跟蹤、查址、尋人等業務，平時為包攬生意，打探隱私，勢必透過種種方式或管道

<sup>28</sup> 見最高法院 88 年台上字第 5741 號刑事判決。

向公務經管單位取得相關資料，前述公職人員因貪圖小利，協助徵信業者代查相關個人資料，以致遭受訟累，足堪同仁引為警訊。

(五) 遭不法集團欺騙代為查詢：

1、案例情節

- (1) 某機關員工張○○於101年3月某日近中午時分，接獲一名自稱該機關前首長的電話，要求查詢被開立無照駕駛罰單之○○○等人（均僅知身分證字號）之駕照是否遭吊銷，張員表示待查證後再回覆，惟對方一再催促致一時失察，遂委請不知情之同事以其帳號密碼進入電腦主機資料庫查詢，並由張○電述提供有關○○○等人之姓名及價籍地址。嗣張○察覺有異，主動向直屬長官報告並經向前所長查證表示未曾電詢，始知受騙<sup>29</sup>。
- (2) 某分局派出所警員李○○於101年2月某日晚間7時至9時，擔服值班勤務，接獲警用分機來電，對方自稱係偵查隊學長○○○，並稱因電腦無法連線登入警政署警政知識聯網E化報案系統，請渠代為協助查詢失竊車輛車籍資料共7筆，並向李員表示，如工作忙碌將改向勤務中心集中查詢所需資料，李員認該員熟稔警察機關內部用語，而誤認該員亦係警職人員，即將所交查之車主相關資料回報該假冒學長者，事後察覺有異，致電該分局偵查隊查證並無其人，李員自覺恐已不慎洩漏民眾個人資料，即主動將上情陳報所長，嗣由該分局調查後函送偵辦<sup>30</sup>。

<sup>29</sup> 見行政院農委會農業金融局網站（網址：<http://www.boaf.gov.tw/public/Attachment/261814491171.doc>）。

<sup>30</sup> 同註17。

## 2、所涉及之法律責任

- (1) 按刑法第 132 條第 1 項規定略以，公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處 3 年以下有期徒刑。（洩漏國防以外之秘密罪）
- (2) 張○○、李○○雖因遭人欺騙洩漏個資，雖未具刑法第 132 條之構成要件故意，或未該當該項罪嫌之構成要件，然其未經查證即行提供相關資訊，仍應追究相關行政責任。

### (六)以協辦業務之便取得系統權限:

#### 1、案例情節

○縣○○鄉公所臨時人員甲與替代役男乙等二人，係依據法令從事公務之人員，負責協辦該鄉公所○○課業務，某甲自民國 94 年 8 月間起，連續利用協助該課業務之便取得數位役男身分證字號，並將取得身分證字號登錄「YAHOO! 奇摩網站」試玩「暗棋」遊戲。另某乙亦利用同樣之方法協辦業務之便，取得該課同仁某系統權限，進入查詢同仁及朋友之個人資料，並利用所得資料破解承辦人員電腦密碼，藉以使用其電腦；朋友部分主要係查詢聯繫資料。甲、乙兩人雖經查證未發現渠等非法從事盜賣資料或提供業者索取不當利益及申請信用卡等行為，但因已違反洩密等相關規定，仍予以行政懲處<sup>31</sup>。

<sup>31</sup>見「臺中市政府使用個人資料查調資訊系統洩密案例」（網址：<http://www.taichung.gov.tw/ct.asp?xItem=182745&ctNode=11326&mp>）。

## 2、所涉及之法律責任

- (1) 本案甲、乙兩人藉由協辦業務機會連續以他人身分證字號進入電腦系統查詢同仁資料之行為，本可能觸犯刑法第 132 條「洩漏國防以外秘密罪」之規定，幸未進而從事盜賣資料或提供業者索取不當利益及申請信用卡等行為，故得從輕發落，實屬萬幸。
- (2) 公務機關人員如依業務職掌經管公務機密資料，理應恪遵作業規定，予以保密，不得洩漏於外，即或在人情壓力下，亦不得破例，否則民眾權益及個人隱私勢將受損，上開案例足堪同仁儆戒。

### (七) 提供關鍵資訊協助冒充警方人員：

#### 1、案例情節

某縣某戶政事所雇員甲負責辦理戶籍登記之櫃檯業務，係依據法令從事公務之人員，渠於某警分局任職期間之同事某乙，在離職後開設代書事務所，因長期為客戶辦理改名，而知悉姓名條例第六條第一項第三款略以：「同時在一縣市內居住六個月以上，姓名完全相同年齡較輕者，得申請改名。」之規定較易申請改名，某乙乃利用曾任職警察熟稔警察機關內部運作規定，向舊時在警分局之同事甲數次詢問「查詢戶籍、口卡號碼」等關鍵資訊<sup>32</sup>。

甲明知該代號係警(戶)政單位列為機密不得對外提供之應秘密事項，竟洩漏予乙，致使乙得據以透過電話冒充警察之名義向多處警察、戶政單位詢問得所欲查詢之同

<sup>32</sup> 見高雄市政府工務局網站(網址：[http://pwb.kcg.gov.tw/upload\\_file/ethic/100-05-.doc](http://pwb.kcg.gov.tw/upload_file/ethic/100-05-.doc))。

姓名人員之人別資料，再詢程序辦理改名，案經檢調單位移送偵辦。

## 2、所涉及之法律責任

本案某甲連續洩漏「查詢戶籍、口卡號碼」予乙之行為，係觸犯刑法第 132 條規定：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處 3 年以下有期徒刑」，而某乙所觸犯者，則係刑法第 158 條第 1 項：「冒充公務員而行使其職權者，處 3 年以下有期徒刑、拘役或 500 元以下罰金」之規定。

### (八) 藉洩漏個資之機索要財物與不法利益：

#### 1、案例情節

某稅捐稽徵處稅務員蔡○○得知友人劉○○欲瞭解其債務人王○○之財產狀況，邀約劉○○前往餐廳，詐稱需支付新台幣五千元費用，調取王○○名下之歸戶財產資料。蔡○○明知違法，仍利用職權填寫「全國財產稅資料總歸戶查詢登記申請單」，以「因案需要」為由，呈不知情之股長及主任核准後，送交電子作業股印製王○○之「歸戶財產查詢清單」。蔡○○當日即將該資料交付劉○○並索得五千元；事後蔡○○數次喝花酒，其費用均要求劉○○付款，計取得價值三萬多元之不法利益。案經轄內調查站主動發掘，移送所轄地方法院檢察署偵查起訴，判處蔡○○有期徒刑四年<sup>33</sup>。

#### 2、所涉及之法律責任

(1) 按刑法第 132 條規定略以：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物

<sup>33</sup> 見司法院政風處網站（網址：<http://www.judicial.gov.tw/ged/2007/?struID=0&navID=24&contentID=21>）

品者，處 3 年以下有期徒刑、拘役或 3 百元以下罰金。因過失犯前項之罪者，處 1 年以下有期徒刑、拘役或 3 百元以下罰金。」

(2) 蔡○○為圖己私之利，知法犯法，竟利用職務之便，調取應保守秘密之納稅人財產資料，誤導民眾以為利用金錢即能取得任何公務機密資料，又蔡○○事後亦利用此事數次向劉○○詐取不法利益，嚴重破壞政府公務人員形象，致遭訟累，深值同仁警惕。

## 二、企業洩漏個資爭議事件：

根據美國 FBI 的一項調查中指出：「內部洩密對大企業造成的損失每年平均為 270 萬美元，外部攻擊平均為 5 萬 7 千美元」差距近 50 倍，自 2003 年起，有關個資洩漏事件層出不窮，而由下述媒體所揭露之訊息似可得知，內部個資洩漏造成的損害遠大於外部攻擊，亦彰顯公務機關對於個資資安維護之重要性，頗值同仁執行業務時加以注意：

表 6：2003 年至 2004 年國內個資洩漏事件彙整表

年度 / 月份	事件摘要
2003/01	財金公司爆發洩密案件，該公司三名工程師與偽卡集團勾結，外洩國內數十家發卡銀行的信用卡「內碼」資料。對於信用卡資料洩密案，財金公司對國內四十九家銀行賠償二億三千萬元。
2003/12	消基會接獲消費者通報，使用 Yahoo 奇摩網站搜尋「病人案件管理系統」，進入中央健保局網站，可點選到許多醫師

	及其診所的資料，醫師所診治過的病人資料也可以看到。「病人基本資料」中出現病人姓名、出生年月日、身分證字號、居住地址及連絡電話等資料，還有實驗室檢查的結果報告。
2004/05	針對逾二千萬筆民眾個人資料外洩，中華電信、遠傳等七家電信業者坦承作業有疏失。根據警政署估計，政府可能得面對七百億元國賠金額。
2004/06	台北市議員藍世聰、劉耀仁指出『名單行銷業者』透過網路販售台北市松山區、信義區部份國小學生、家長資料，每筆資料只賣一元。業者聲稱掌握三十萬筆學生資料。

**表 7：2004 年至 2005 年國外個資洩漏事件彙整表**

年度/月份	事件摘要
2004/02	日本網際網路「雅虎 B B」公司外洩四百五十萬筆個人資料，引起社會指責，雅虎 B B 以每筆賠償五百日圓（約合新台幣一百六十元）平息此事件，總計賠償二十三億日幣（約合新台幣七億元）。雅虎 B B 公司因此而財務困難。
2005/01	東京迪斯奈樂園「終年通行證」的客戶資料疑外洩，歹徒要求贖金，否則將公開這些資料。園方針對客戶資料洩密事件向十四萬客戶鄭重道歉。
2005/02	著名的 NTT DoCoMo 公司發生醜聞，大約 24,600 個客戶的資料洩露出去。資料可能是由內部員工從一個被認為很安全的房間竊出，只有 254 名員工可以進入此房間。房間 24 小時 6 支攝影機監控，員工必須先登記，並且經過瞳孔掃描，驗明身份，方可進入。
2005/03	柏克萊加州大學警告，該校研究所入學許可辦公室的一台筆

	記型電腦遭竊，可能導致超過 9 萬 8 千人的個人資料外洩。
--	--------------------------------

## 陸、本府使用個人資料資訊系統專案稽核成果：

### 一、專案稽核概況：

#### (一) 專案稽核計畫：

由本處訂定(詳附件)。

#### (二) 受稽核機關(或單位)：

本府掌管個資之重點機關包括警察局、衛生局、地方稅務局、民政局、地政局暨所屬等 52 個機關(或單位)。

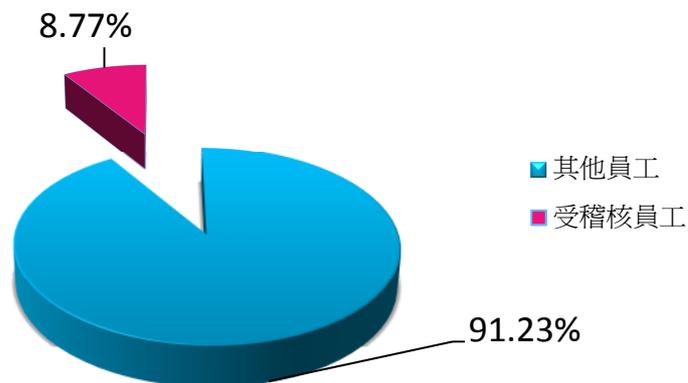
#### (三) 稽核項目：

使用個人資料資訊系統查核個人資料相關 47 個項目。

#### (四) 稽核人數：

前揭 5 個機關本次稽核員工 482 人次，該等機關正式及約聘僱人員統計至 102 年 6 月底止計 5499 人(資料來源：人事處)，稽核人數占全體員工比例約為 8.77%。

專案稽核人數占本府全體員工比例



(五) 稽核資料筆數：

1250 筆。

(六) 發現缺失：

計 52 項。

二、各機關專案稽核項目及稽核件(人)數：

(一) 本府地方稅務局：

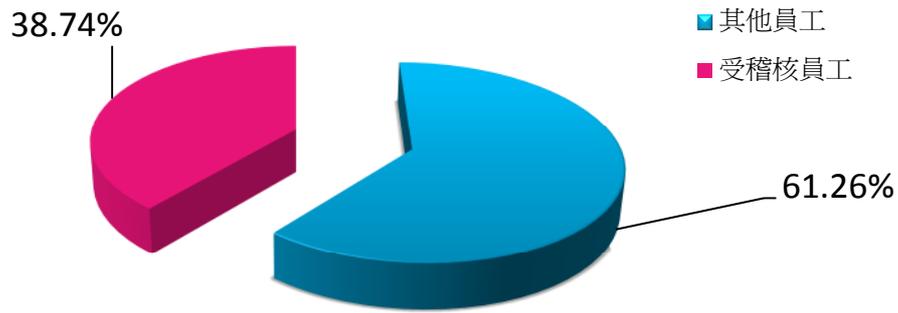
1、專案稽核項目計 10 項：

- (1) 系統使用權限管理。
- (2) 是否依規定查詢納稅義務人個人資料。
- (3) 辦理員工教育訓練相關員工個人資料保密作為。
- (4) 利用網路辦理線上申辦稅務之保密作為。
- (5) 委外業務保密作為。
- (6) 電子郵件涉及個人資料傳送保護作為。
- (7) 影印及傳真涉個人資料保護作為。
- (8) 人事陞遷考核及甄審涉個人資料保護作為。
- (9) 單位業務涉個人資料之紙本保管及維護。
- (10) 其他一個資保護相關事項。

2、稽核件(人)數：

總局各科室及中壢、楊梅、大溪三個分局業務承辦同仁，自 101 年 7 月 1 日起到職新進人員全數列入複核，總計稽核 129 人次(筆)資料，該局暨所屬正式及約聘僱人員統計至 102 年 6 月底止計 333 人(資料來源：人事處)，稽核人數占全體員工比例約為 38.74%。

專案稽核人數占該局全體員工比例



(二) 本府衛生局：

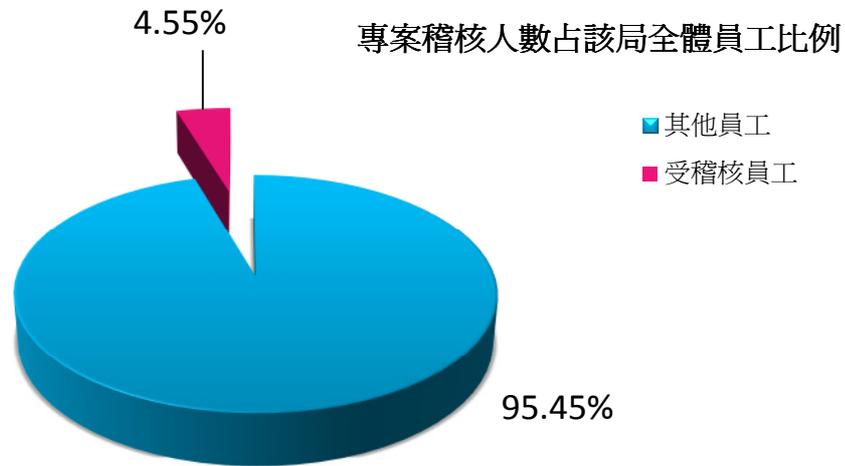
1、專案稽核項目計 13 項：

- (1) 系統使用權限管理。
- (2) 是否依規定查詢個人資料檔案。
- (3) 個人資料之紙本保管及處理。
- (4) 資安教育訓練。
- (5) 員工教育訓練相關員工個人資料保密作為。
- (6) 查閱個資之作業程序。
- (7) 電腦報廢程序。
- (8) 受理檢舉案件之保護檢舉人作為。
- (9) 委外業務保密作為。
- (10) 電子郵件涉及個人資料傳送保護作為。
- (11) 人事陞遷考核及甄審涉個人資料保護作為。
- (12) 單位業務涉個人資料之紙本保管及維護。
- (13) 其他一個資保護相關事項。

3、稽核件(人)數：

計稽核 13 個衛生所，稽核系統使用者 21 人，使用者帳號查詢筆數 789 筆資料，該局暨所屬正式及約聘僱人員

統計至 102 年 6 月底止計 461 人(資料來源：人事處)，稽核人數占全體員工比例約為 4.55%。



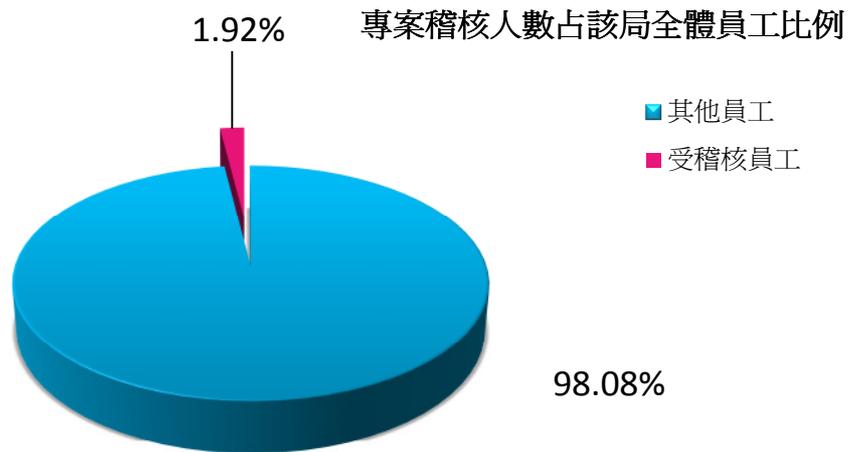
### (三) 本府警察局：

#### 1、專案稽核項目計 8 項：

- (1) 資料查詢程序及紀錄。
- (2) 系統使用權限管理及稽核。
- (3) 防制機敏性資料外洩執行情形。
- (4) 硬軟體管理維護紀錄。
- (5) 網路管理。
- (6) 個人電腦防毒軟體版本更新。
- (7) 管理者權限收回等事宜。
- (8) 機敏性業務單位資訊安全檢查項。

#### 2、稽核件(人)數：

計稽核該局所屬 10 個分局及 5 個警察大隊，計實施資安督考 72 人次(筆)資料，該局暨所屬正式及約聘僱人員統計至 102 年 6 月底止計 3748 人(資料來源：人事處)，稽核人數占全體員工比例約為 1.92%。



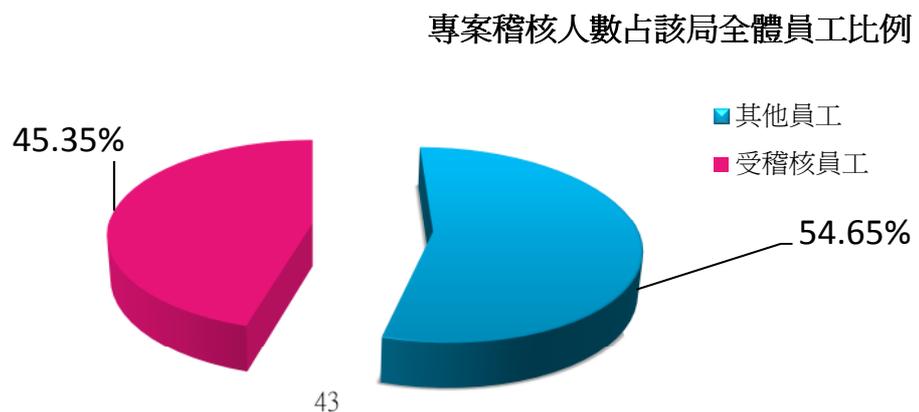
(四) 民政局：

1、專案稽核項目 3 項：

- (1) 已成案者之申確認係因公查詢。
- (2) 未成案者之資料流向。
- (3) 未成案之原因。

(二) 稽核件數：

計稽核該局及 13 個戶政事務所，計訪談機房管理 15 人，稽核案件 190 人次(筆)資料，該局暨所屬正式及約聘僱人員統計至 102 年 6 月底止計 419 人(資料來源:人事處)，稽核人數占全體員工比例約為 45.35%。



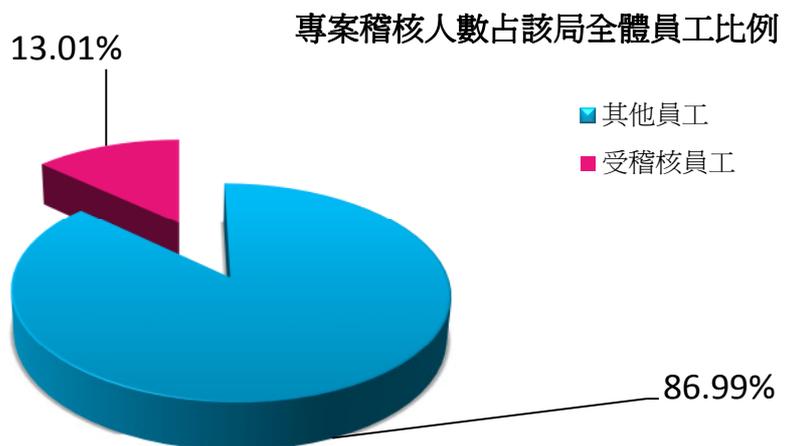
(五) 地政局：

1、專案稽核項目 13 項：

- (1) 系統使用權限管理。
- (2) 是否依規定查詢個人資料檔案。
- (3) 個人資料之紙本保管及處理。
- (4) 資安教育訓練。
- (5) 員工教育訓練相關員工個人資料保密作為。
- (6) 查閱個資之作業程序。
- (7) 電腦報廢程序。
- (8) 受理檢舉案件之保護檢舉人作為。
- (9) 委外業務保密作為。
- (10) 電子郵件涉及個人資料傳送保護作為。
- (11) 人事陞遷考核及甄審涉個人資料保護作為。
- (12) 單位業務涉個人資料之紙本保管及維護。
- (13) 其他-個資保護相關事項等 13 項。

2、稽核件數：

計稽核所屬 7 個地政事務所 70 人次(筆)資料，該局暨所屬正式及約聘僱人員統計至 102 年 6 月底止計 538 人(資料來源：人事處)，稽核人數占全體員工比例約為 13.01%。



### 三、各機關專案稽核發現之相關缺失：

計「未落實填寫查詢用途欄」、「未依規定申請核准使用及造冊列管」、「查詢用途不明」等項如下表：

**表 8 各機關專案稽核發現之相關缺失**

1. 電腦安裝無版權軟體。
2. 未設置行動電腦每日更新稽核簿冊
3. 領用行動電腦載具未完整登錄載具全碼。
4. 電腦共用資料夾但未設定存取密碼進行全線管控。
5. 電腦未安裝防毒軟體。
6. 個人電腦未停用管理者(Administrator)權限情形及個人電腦疑似遭植入後門程式情形。
7. 電腦中發現有無版權電影檔案及領用行動電腦載具為完整登錄載具全碼。
8. 發現有電腦管理者帳號密碼張貼於螢幕上、個人電腦未依規定使用 AD 帳號登入。
9. 發現同仁於非勤務時間查詢各項個資資訊系統。
10. 普遍未落實填寫查詢用途欄。
11. 普遍未將單位內具查詢個資權限人員整理成冊，且未定期更新備查。
12. 各單位雖均能設置實體隔離電腦設備，惟機敏性資料未能落實存放於實體隔離設備中。
13. 各單位使用可攜式儲存媒體(USB 隨身碟等)情形十分普遍，惟普遍未依規定申請核准使用及造冊列管。
14. 仍發現有未確實收回管理者(Administrator)權限情形，且未加入 AD 群組，易遭受惡意程式攻擊。

15. 針對查詢條件異常、高查詢量帳號或高風險違紀對象稽核結果未於聯合勤教宣導，無紀錄可稽。
16. 未請離職人員填寫系統權限刪除單，亦未及時將離職人員名冊傳真陳報報。
17. 委外廠商維護合約沒有保密切結的條款或保密切結書。
18. 主機房進出表部份各所表格不一，部份沒有填寫，有填寫部份沒有經主管核章，無填進出入主機房的時間及缺少主機房管理者、主管核章的地方。
19. 報廢電腦的硬碟處理回收流程有誤，少做硬碟 format 資料的動作，另無填寫廢品紀錄單。
20. 兼辦資訊管理人員並無執行定期抽查「戶役政資訊系統」資料查詢及異動紀錄此一作為。
21. 發現運用該系統查詢有未事前經核准，且未於查詢申請表登記，查詢資料無相關依據可供釐清是否因公務需要查詢。
22. 未事前經主管核准即查詢，而於查詢後再核章程序錯誤之情形，亦無將書面依據附於查詢申請表。
23. 各類如 TB 等個案資料卻放置於開放架上，對個人資料之紙本保管及處理未善盡，且查詢人員於列印個人資料後交各地段時亦無簽收之程序。
24. 針對查閱個資之作業程序，實地稽核結果發現查閱個人資料而未列印者，部份未登記申請案號或申請事由，且未逐筆紀錄，1 身分字號或姓名查詢多次僅登記 1 筆，申請表格欄位未有註明有無列印。
25. 電腦報廢程序，電腦報廢移交前，有部份機關未將

電腦內所有儲存資料全部刪除，而僅將硬碟拆除搗碎。

26. 電子郵件涉及個人資料傳送保護作為部份，發現同仁以電子郵件傳送有關機密或個資資料之附加檔案都未加密。
27. 申請事由查詢條件未填依據或檢附案由。
28. 內政部戶役政電子閘門系統查詢申請及紀錄表未編流水號名。
29. 發現部分單位之人員雖已調職，但帳號仍可正常使用；另部分單位帳號異動申請單內有關離職人員申請日期、註銷原因、使用期間等資料亦未填註，有失完整。
30. 少數受檢單位「磁帶備份紀錄單」，未依分層負責明細表規定由單位主管核閱，而僅由承辦人員核章，與現有規範相間。
31. 發現部分日誌及人員管制簿內，出現漏填維修廠商進出時間之情事。
32. 經實施稽核結果，多數受檢單位均能定期辦理抽查，且承辦人員均能依規定填寫申請事由及目的，然仍有少數人員於查詢「戶役政資訊系統」時，所填寫之登記原因有誤；另經抽查「免書證免謄本系統」，亦發現少數案件查詢目的書寫有誤，顯示部分同仁於執行個資查詢作業時，仍有便宜行事之心態。

#### 四、行政懲處或函送情形：

○所 A 員使用戶役政資訊系統未依規定申登資料，經政風室調閱管理系統 log 檔發現該所於稽核期間使用前揭戶役政資訊系統計 32 筆查詢紀錄，其中 31 筆無申請事由及作業時間等登記資料，A 員顯未依作業管理規範進行查詢，且 log 檔自 100 年 1 月 4 日起紀錄查詢民眾個資等情事，A 員坦承非因公務查詢，業經該機關以違反個人資料保護法核予申誡 1 次並函送司法機關查察。

### 柒、策進措施與建議事項

#### 一、制度面：

##### (一) 全面落實電子化作業制度：

各機關處理公文案件數量龐大且人力有限，故在無法增加複核機制情形下，為迅速便民要求，惟有落實電子化作業制度，除了由民眾藉由網路申報辦外，另受理申辦機關得直接以網路查證相關資料，如此可以減少洩密情事之發生。

##### (二) 建立系統預警機制：

遇有相同情形次數較多且屬異常情形高危險群者，例如同一人於一年內以「土地利害關係人」身分申請其他土地共有人戶籍謄本案件超過 3 件者，可在建制警示承辦人應先查詢地籍資料確認其文件之真實性等機制，即可避免發生類此遭冒領大量戶籍謄本案件發生。

##### (三) 增加使用查詢紀錄檔功能或延長保存時效：

因無個人使用查詢紀錄檔功能，故無法提供使用紀錄資料，致無法進行內部稽核，恐造成弊端；另紀錄查詢資料之 log

檔雖具有證明查閱內容、人員及使用電腦設備之證明力，且係屬阻嚇違規查閱之利器，如保存期限天數較短者，實有不足，應延長保存期限。

(四) 落實職務輪調制：

按職務輪調除增加同仁知能、工作士氣、服務品質、工作氣氛及行政效率外，最重要在於得強化內控機制，健全秩序，避免久任一職之弊端，實有防弊之利。

(五) 建立系統需輸入申請人資料之機制：

承辦人受理申請案後即載入申請人資料，再進入查證，如此不僅保有完整記錄，方便內部稽核，並能產生阻嚇效果，避免承辦人有僥倖之心態而誤蹈法網。

(六) 權限之使用應配合個人自然人憑證：

目前之權限僅針對申請者之帳號及密碼管理，或雖有搭配自然人憑證使用，惟係以機關名義申請，故如有發生洩密情事者，無法真正釐清責任歸屬，故建議除了以帳密管理外並賦予應以使用者之個人名義之自然憑證方得使用。

(七) 辦理定期或不定期稽核作業：

由於個人資料保護法業於 101 年 10 月 1 日施行，為避免影響民眾個資權益，各機關可透過訂定計畫辦理定期或不定期稽核，俾以防杜可能弊端。

二、執行面：

(一) 加強人員平時考核：

對於承辦同仁之平時考核應予以落實，並對於如有生活異常之人員及收支異常人員應注意其作業情況，必要時予以調整職務。

(二)落實人員調動情形辦理帳號及權限異動：

於承辦同仁職務有異動時，除應即時進行帳號及權限調整外，另得定期辦理清查，以免遺漏而不自知，間接導致資安漏洞之產生。

(三)加強落實機房之人員與物品管制：

部分機關因空間不足未有獨立之機房者，惟仍有必要以隔離或遮蔽方式將主機隔離防護以維資安；有獨立機房之機關，雖電腦機房及伺服器以備網路使用有設置門禁管理，管控人員進入，惟仍發現可能有貪圖方便，致出現漏填維修廠商進入事由及離去時間之情事。

(四)對於硬碟或隨身碟報廢應落實以物理性破壞：

電腦硬碟或隨身碟報廢之處置作法，應施以物理性破壞，以免報廢後硬碟或隨身碟所載資料不慎流出，引發後續爭議。

(五)加強人員教育訓練：

個人資料保護法業於 101 年 10 月 1 日正式施行，其中有許多觀念是先前法令所沒有的，故可加強教育訓練，使同仁得以了解相關法令，藉以擴大宣導效能並增加同仁對實際情境的感受及引起學習動機和興趣。

(六)加強資訊軟硬體設備：

1、購置 LOG 日誌管理器：

購置 LOG 日誌管理器俾有效提升系統日誌管理與舉證能力、HP-ArcSight LOG 日誌管理器可作為日誌管理之工具輔助，並提出詳盡資訊供事後追蹤與資安漏洞補強。

2、購置資產管理系統：

提供資訊設備財產管理員控管機制，禁止使用者安裝未經核准軟體及硬體，以降低資料外洩風險強化資安控管。

3、購置預防資料外洩系統：

為加強個資外洩防制措施與紀錄證據保存機制，以個資保護系統導入服務，建構個資事故管理處理機制，降低因事故發生造成損失。

## 捌、結語

對於擁有大量個人資料的公務與非公務機關而言，建立個人資料的保護權責，已不再是「資訊單位」的責任，若僅限於機房實體防護、主機與應用系統、資料庫定期弱點掃瞄與滲透測試就能確保個人資料的安全性，當然，上述工作實有其存在之必要性，相關取得、持有、操作、傳遞、儲存與銷毀的同仁，都必須落實合乎規定，稍有不慎，則機敏的個人資料就會外流至惡意或無惡意的組織或個人，資安事件所衍生之罰鍰與處分以及連帶可預期組織形象的損失均在考驗組織面對此一議題所需投入的精力與資源，然而個人資料保護之要求，已是各個機關團體或組織無可迴避的重要業務，而個資法亦課予公務機關及私人企業許多義務與罰則，因此本府掌理民眾大量個資之警察、地

政、民政、衛生及稅務等機關員工查詢、處理或利用個人資料時，應更為謹慎，以免不慎觸法。

另現今電子化政府已是當前為民服務品質提昇的重要指標，而跨機關資料的整合、傳遞則是目前發展電子化政府最重要的議題。在便民的同時，應藉由機關內外相關之資安維護措施，提升資訊安全的防護能力，促使機關同仁對民眾基本資料保密工作之認知與重視，並強化個資「時時保密」、「處處防護」之觀念，實為嚴肅不可忽視的重要課題。

## 附件：桃園縣政府 102 年使用個人資料查詢資訊系統專案稽核計畫

### 壹、依據：

- 一、 行政院及所屬各機關資訊安全管理要點。
- 二、 法務部廉政署 102 年 02 月 22 日廉政字第 10207000380 號函。
- 三、 本府「102 年度政風工作計畫」及各機關資訊安全作業等相關規定。

### 貳、目的：

為確保本府各機關人員使用個人資料相關查詢資訊系統具合法與正當性，防範個資外洩，維護民眾隱私、財產等憲法基本權利，落實資訊安全與公務機密之管理，爰訂定本專案稽核計畫。

### 參、稽核之期間與對象：

自 101 年 10 月 1 日至 102 年 5 月 31 日止，本府所屬機關、委外人員就相關資訊系統個資資料之查詢、蒐集、利用、處理等情形。

### 肆、稽核之機關：

#### 一、掌管民眾個資相關資訊系統之重點機關：

本府地方稅務局、警察局、民政局、地政局、衛生局等所屬機關為本計畫應稽核機關。

#### 二、其他機關：

視機關資訊系統掌理民眾個資之廣度或密度，自行決定依本計畫辦理專案稽核。

### 伍、稽核方向：

各機關應就資訊系統查詢、蒐集、利用、處理個資之程序、權限、目的、紀錄、證明文件及相關管理情形，訂定專案稽核計畫、表格據以辦理。

### 陸、稽核人員與教育訓練：

#### 一、 稽核人員：

由各機關政風及資訊人員組成稽核小組辦理專案稽核。

#### 二、 期前教育訓練：

為期各機關之稽核人員熟稔「個人資料保護法」等相關法令，由本府政風處及地方稅務局於 102 年 3 月底前共同辦理 2 場次「個人資料保護法令與實務」專題講座，參加人員為本府各機關政風及稅務人員。

### 柒、稽核結果之陳報：

各機關稽核結果與改善情形由本府政風處彙整專報陳 縣長核定。

### 捌、稽核經費：

本專案稽核經費，於各機關資訊作業項下相關經費支應。

### 玖、本專案稽核計畫奉 縣長核定後實施，修訂時亦同。