國立臺灣大學社會科學院國家發展研究所

碩士論文

Graduate Institute of National Development
College of Social Sciences
National Taiwan University

Master Thesis

敏感性個人資料保護之研究

A Study of Sensitive Personal Data Protection

蔡秉錡

Charles Ping-Chi Tsai

指導教授：湯德宗 博士

Advisor: Dennis T. C. Tang, S.J.D.

中華民國 101 年 6 月

June, 2012

誌謝

論文初稿是我在台大國家發展研究所修習「公法學專題」的課堂報告。撰寫期間，適逢我國個資法修正，新增特種資料（敏感性個資）之規定，正好使本文能夠順應潮流、符合時事，這是始料未及之事。希望本文研究，對於掌握敏感性個資之概念與訂定相關規範有所助益。

完成本篇論文，首要感謝的是我的指導教授，司法院大法官　湯德宗先生。湯大法官是我在 2001 年於東吳法律系修習「中華民國憲法」的授課教授，修業期間深受湯大法官的學思影響，開展我對於公法學的興趣與熱忱，也因此促使我畢業後報考國立臺灣大學國家發展研究所，順利錄取並有幸成為湯大法官的指導學生。同時，中央研究院法律學研究所籌備處於 2004 年成立，湯大法官時任法律所籌備處主任兼研究員，給我工讀與學習機會，讓我到法律所去協助處理行政庶務。因此自 2004 年開始，我一路從工讀生、編輯室校稿助理、法律所獎勵補助研究生、院內深耕計畫兼任助理及最後的專任助理，七年來在法律所歷練成長，這是我人生中不可多得的經驗，但這一切都要感謝十餘年來對我耐心提拔的湯老師。尤其，湯大法官對我的論文細心逐字斧正，公務繁忙之餘仍每週撥空與我討論爭點疑義，獲益良多，僅能於此略記數語，以表達謝意。此外，本文另外兩位審查老師，本所劉靜怡教授，與東吳大學法律學系主任林三欽教授，對本文議題有深刻且獨到的研究，感謝兩位老師的指點與建議。

我要感謝我的女朋友－嘉儀，遇見她是我人生最好的際遇，她全心一意陪伴我，默默督促我盡快完成，是這篇論文的潛在推手。我願在將來時光裡，與她相互扶持、攜手同行。同時，也感謝嘉儀的家人，不時給我關心與鼓勵，讓我在離鄉背井求學之時，仍能感受到親情與家人的關懷。

此外，也要感謝中研院法律所的學長姐、學弟妹，包括：黃建普、黃慧儀、陳家瑀、王漢民、大嘴（陳冠宇）、李佳臻、劉宗翰、陳姵蓉、李佩容、鄭凱尉等好友，你們豐富了我過去七年在法律所的回憶；研究所同窗：蘇緯政、廖悅涵及學弟楊大維；東吳的同學與學弟：劉蕙瑢、鐘惠盈與吳旻訓，對本文的完成提供了不等的協助，一併在此致謝。

最後，要感謝我的家人。我的父母親不曾給我壓力。他們默默守候我，看著我步步前進。將來，希望我能不負他們期望，服完兵役後繼續前往國外留學，無愧天賦，以此回報。同時，謝謝我的妹妹，一直在家鄉陪伴父母，代盡兄責，由衷感激。

中文摘要

2011 年，我國通過新修正之個人資料保護法，第六條第一項規定，有關醫療、基因、健康檢查、性生活與犯罪前科之個人資料，為敏感性個人資料，或謂特種資料。

個人資料是否屬於敏感性個人資料，應考量資料之性質，並以法律列舉之方式定義。個人資料保護法目前列舉之類別，有四類與健康相關，且遺漏病歷資料，類別有待重整。指紋雖屬生物辨識資訊，具敏感性個人資料之特質，惟目前各國立法仍缺乏共識，暫時無須列為敏感性個人資料。

敏感性個人資料因性質特殊，不當蒐集、處理或利用容易侵害個人資訊隱私，故各國原則上率皆禁止蒐集、處理或利用之，例外始得蒐集、處理或利用。個人資料保護法規定四種得蒐集、處理或利用敏感性個人資料之例外情形，現行各款規定有欠明確，且四種情形與各國立法例相較為少，將來可新增「當事人書面知情同意」、「基於醫療行為」或「重大公益所必要」之例外條款。

個人資料保護法對敏感性個人資料之保護，尚有不足，尤其關於公務機關或非公務機關是否須履行通知義務，以及特定目的外利用之情形，適用上仍有疑義，應修正補強。

關鍵字：敏感性個人資料、特種資料、個人資料保護法、歐盟個人資料保護指令、個人資料保護原則

Abstract

Sensitive Data or Sensitive Information is a sub-set of personal information and is given a higher level of protection under Personal Information Protection Act(PIPA) Art.6(1). The definition of Sensitive Data(special categories of data) in the PIPA refers to information about an individual's: medical treatment, genetic information, sexual life, health examination and criminal record.

Any Information can be considered to be sensitive, depending on the nature. The better approach to define sensitive data is specifically enumerating special categories of sensitive data by Law. Almost all Sensitive data enumerated in current PIPA is about medical information and lacks medical record, therefore the list should be consolidated and amended. Fingerprint is biometric information which can be considered sensitive, but there is no legislation in other country, so it may not be added to the list temporarily.

PIPA prohibits Government agency or Non-government agency from collecting, processing and using sensitive data unless at least one of the conditions(exemption) set out in Art.6(1) is fulfilled. However, the definition of the exemptions is vague and ambiguous. The types of the exemptions defined in PIPA are less than legislation in other country as well. Therefore this thesis suggests that PIPA should be amended and many other conditions, such as "data subject's informed consent", "for medical purposes" exemption, "for public interest" exemption and "in order to protect the vital interests of another person" exemption should be added.

Although PIPA gives higher level of protection to sensitive data, it does not specifically state whether Government agency or Non-government agency should notice data subject before collecting sensitive data, or whether sensitive data can be used for secondary purpose. It should be amended immediately before the date for enforcement of the Act.

Keywords: sensitive data, sensitive information, special categories of data, personal data protection, data protection principle, Personal Information Protection Act

目次

圖次

表次

縮語表

個資法＝ 個人資料保護法(99/05/26)

個資法施行細則草案＝ 個人資料保護法施行細則修正草案(100/10/26 公告)

舊個資法＝ 電腦處理個人資料保護法(84/08/11)

歐盟個資指令＝ 歐盟個人資料保護指令(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data）

歐盟個資指令修正案＝ 歐盟個人資料保護指令修正提案（Data Protection Directive (95/46/EC) Proposals for Amendment made by Austria, Finland, Sweden and the United Kingdom, Explanatory Note, September 2002 Special Categories of Data Proposal）

OECD 個資綱領＝ OECD 個人隱私與跨境個人資料流通保護綱領(Annex to the Recommendation of the Council of 23rd September 1980: GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA)

歐盟個資公約＝ 歐盟保護個人關於自動化處理個人資料公約(CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, Strasbourg, 28.I.1981)

個資規範＝ 聯合國規範電腦化個人資料檔案指導綱要(Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 44/132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989))

加拿大個資法＝ 加拿大個人資訊保護暨電子文件法(Personal Information Protection and Electronic Documents Act 2000, PIPEDA)

澳洲法改會＝ 澳洲法律改革委員會(Australian Law Reform Commission)

第一章　緒論

壹、研究動機

1997 年 5 月 21 日，戶籍法草案修正公布。其中，第 8 條規定年滿十四歲之人民請領國民身份證應按捺指紋，[1]惟當時身分證已自 1985 年起陸續換發，且建立指紋檔案事涉繁瑣，幾經討論後經行政院決議暫不施行，[2]嗣後並四度受到監察院糾正。[3]2005 年 4 月 6 日，行政院指示自同年 7 月 1 日起換發新式國民身分證，全體國民須按捺指紋始得領取。立法委員賴清德等人，認上開條文違反憲法第 22 條及第 23 條之規定，爰依司法院大法官審理案件法第 5 條第 1 項第 3 款，[4]於同年 6 月 6 日向司法院大法官聲請解釋，同時並聲請「急速處分」，以宣告係爭條文（戶籍法第 8 條全項）暫時停止適用。2005 年 6 月 10 日，司法院大法官先作成釋字第

---

[1] 戶籍法(96/05/21)第 8 條第 1 項：「人民年滿十四歲者，應請領國民身分證」；第 2 項：「未滿十四歲者，得申請發給。依前項請領國民身分證，**應**捺指紋並錄存。但未滿十四歲請領者，不予捺指紋，俟年滿十四歲時，應補捺指紋並錄存」；第 3 項：「請領國民身分證，不依前項規定捺指紋者，**不予發給**」。

[2] 相關過程可參見本案理由解釋書，或參見曾珮瑩，《全民指紋建檔爭議之研究-以 94 年換證為例》，銘傳大學公共事務學系碩士論文，頁 71-80（2008 年）。

[3] 第一次糾正，參見監察院公報，2196 卷，頁 301-306（1999 年 2 月 10 日）；第二次糾正，參見監察院公報，2232 卷，頁 2299-2307（1999 年 10 月 20 日）；第三次糾正，參見監察院公報，2310 卷，頁 76-77（2001 年 04 月 18 日）與監察院公報，2312 卷，頁 1-6（2001 年 05 月 02 日）；第四次糾正，參見監察院公報，2316 卷，頁 54-55（2001 年 05 月 30 日）與監察院公報，2317 卷，頁 11-19（2001 年 06 月 06 日）。各次糾正之重點摘要，可參見曾珮瑩，前揭（註 2）文，頁 92。

[4] 司法院大法官審理案件法(82/02/03)第 5 條第 1 項第 3 款：「有左列情形之一者，得聲請解釋憲法：…三、依立法委員現有總額三分之一以上之聲請，就其**行使職權**，適用憲法發生疑義，或**適用法律**發生有牴觸憲法之疑義者」。本案同時引起大法官應否受理申請之爭論，主要參見廖義男大法官「協同意見書」、楊仁壽大法官「不同意見書」以及謝在全大法官「不同意見書」。

599 號解釋，暫停戶籍法第 8 條第 2 項及第 3 項之適用，並駁回聲請人就同條第 1 項之暫時處分聲請。2005 年 9 月 28 日，司法院大法官就前述已暫時停止適用之戶籍法第 8 條第 2 項及第 3 項，作出釋字第 603 號解釋。

釋字第 603 號解釋，認為「根據戶籍法第 8 條第 2 項、第 3 項，未按捺指紋者不予換發國民身份證」之規定係屬違憲。解釋文謂：「指紋乃重要之**個人資訊**，個人對其指紋資訊之自主控制，受資訊隱私權之保障」。理由解釋書中復謂：「指紋係個人身體之生物特徵，因其具有人各不同、終身不變之特質，故一旦與個人身分連結，即屬具備**高度人別辨識**功能之一種**個人資訊**。由於指紋觸碰留痕之特質，故經由建檔指紋之比對，將使指紋居於開啟完整個人檔案鎖鑰之地位。因指紋具上述諸種特性，故國家藉由身分確認而蒐集個人指紋並建檔管理者，足使指紋形成得以監控**個人之敏感性資訊**」。[5]本號解釋多數意見認為指紋可合理聯結、揭露個人資訊，故屬「個人之敏感性資訊」，惟對於該概念之特徵與內容，本號解釋文及理由書並未多所著墨。[6]

對此，有三位大法官，表達不同看法。許玉秀大法官之「協同意見書」認為是否得強制按捺指紋，須取決於「指紋是否為敏感資訊」。氏認為「所謂資訊的敏感度，就是該資訊如果脫離個人控制，可能對個人造成的損害有多大，也就是**資訊的抽象危險性**有多高的問題」。指紋對於保護人身安全，可作為有利資訊，但對於控制人民之制度，又為負面資訊，是故，指紋不屬於絕對敏感資訊，**僅具備「相對的敏感度」**，其敏感度在於它的「程序性質」**可以辨識人別**，辨識的精確度愈高，

[5] 參見司法院大法官釋字第 603 號解釋。

[6] 林子儀大法官於本案之「協同意見書」嘗提及：「...多數意見似主張指紋之性質非如**醫療紀錄、性傾向、宗教信仰或政治立場**般敏感...」表達本案大法官曾就「指紋」之性質予以討論，同時約略引出「敏感性個人資料」之概念，惜未能就「敏感性個人資料」一詞於解釋理由書中釋示。

抽象危險性愈高。一旦確認資料屬性，個人即失去自身資訊之自主控制，此為指紋資訊之敏感度。

余雪明大法官之「部分協同部分不同意見書」則直接論述指紋之意義。氏認為指紋為個人資訊之一種，指紋與隱私權無關，指紋僅為「**中性之身分辨識工具**」，且**不能因指紋所聯結之資訊本身敏感**，而**認為指紋亦為敏感性資訊。所應禁止或限制者為該項敏感資訊之蒐集，而非指紋或姓名**。[7]余大法官舉比較法作為例證，歐盟個人資料保護指令（下稱「歐盟個資指令」）[8]與英國資料保護法(UK Data Protection Act 1998)中，有關敏感性個人資訊的定義，並未包括指紋。此見解與多數意見截然不同，引起相當討論。[9]

林子儀大法官之「協同意見書」，則對「指紋為中性資訊」持不同意見。首先，林大法官認為**資訊隱私權欲保護之對象應包括指紋**。因為依現今資訊科技之發展，過去所無法處理之零碎、片段、無意義的個人資料，於今已能快速串連、比對歸檔與系統化。當大量個人之中性資訊群聚時，個人之私密資料將呼之欲出。是故，隱私權之保障範圍應隨之擴張至「非私密」或「非敏感性」之個人資料保護，不限於個人秘密不受揭露的自由。其次，指紋並非不帶私密性或不具敏感性

---

[7] 城仲模大法官，於「協同意見書」也表達類似的見解：「**指紋本為中性之資料，單純知悉**個人之指紋並**無法透露任何訊息**，蒐集指紋對於隱私權的影響如何，端視指紋在**個案中的用途**而定」。

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Art.8 [*hereinafter* Directive 95/46/EC].

[9] 參見李建良，〈「捺指紋規定釋憲案」鑑定意見書〉，《台灣本土法學》，73 期，頁 41-44（2005 年 8 月）；李震山、黃昭元、蔡宗珍、顏厥安，〈釋字第 603 號（全民指紋建檔案）評釋〉，《台灣本土法學》，75 期，頁 115-116（2005 年 10 月）；廖元豪，〈高深莫測，抑或亂中有序？—論現任大法官在基本權利案件中的「審查基準」〉，《中研院法學期刊》，2 期，頁 243-244（2008 年 3 月）；林宛怡，《以犯罪偵查為目的之 DNA 資料保存-以歐洲人權公約第八條為中心》，國立政治大學法律學研究所碩士論文，頁 142-143（2009 年 12 月）。

的中性資訊。蓋**指紋具有許多適用於人別辨識與認證之特性**，國家得藉由指紋以掌控國民行蹤。因此，指紋實為敏感性之個人生物資訊。

綜上所述，大法官們對於「指紋」究竟是否為敏感性個人資訊仍有不同見解。本文認為，原則上可分為兩種立場，第一，多數認為：藉由掌握指紋，得以合理聯結或揭露個人資訊，是故指紋為得以監控個人之敏感性資訊；第二，余雪明大法官認為：指紋僅為一識別工具，不具有任何敏感性，並不因其得與其他敏感性個資聯結，而視為敏感性個人資料。細繹問題爭點，係對於敏感性個人資訊之**定義**理解不同所致。第一種見解，顯然著重取得資訊後的「**效果**」，認為指紋其得以與大量、敏感之個人資訊聯結，因而屬「敏感性資訊」；第二種見解，則著重於資訊（指紋）自身的「**內容**」是否屬於「敏感性資訊」而定。對此差異，本文作者不禁產生懷疑，究竟敏感性個人資訊指涉為何？其與一般個人資料有什麼不同？此為本文主要問題意識，以下將以此開展本文架構。

貳、研究目的

一、何謂敏感性個人資料？

本文針對「敏感性個人資料」之保護，進行比較研究。[10]首先討論「敏感性個人資料」之定義與類別。各國個人資料保護法，對於敏感性個人資料之定義不一。「歐盟個資指令」第 8 條規定，「敏感性個資」係限於「顯示**種族血緣、政治意向、宗教或哲學信仰、工會會員資格**之個人資料及涉及**個人醫療或性行為**等資料」。[11]同屬歐盟法規範下之英國，定義「敏感性個資」係指該資料揭露以下事項：「資料主

[10] 鑑於釋字第 603 號解釋與「個資法」之用語並不相同，前者稱為「敏感性資訊」，後者則稱「特種資料」，為避免誤解、統一用語，本文以下統稱「敏感性個資」。

[11] Directive 95/46/EC Art.8.1

體之種族或血緣、政治意見、宗教或類似信仰、工會會員資格、生理與心理健康情況、性生活、有罪指控與起訴調查程序」。[12]至於其他國家，例如澳洲隱私法(Privacy Act 1998)規定敏感性個資為：「揭露種族血緣、政治意見、政治團體會員資格、宗教信仰、哲學信念、專業協會會員、工會資格、性傾向與行為、刑事記錄與有關個人之健康資訊」。[13]

準此而言，各國所謂之「敏感性個資」，係取決於該資訊所揭露之「內容」，並非以該資訊是否得與其他（敏感性）個人資訊聯結為斷。此立場與釋字第 603 號解釋中所採取之見解，並不相同。我國舊法「電腦處理個人資料保護法」（下稱「舊個資法」）未規範敏感性個資。2010 年 5 月 26 日，新修正公布之「個人資料保護法」（下稱「個資法」）第 6 條，規定「有關**醫療、基因、性生活、健康檢查**及**犯罪前科**之個人資料」不得蒐集、處理及利用之，此為我國法上「敏感性個資」，惟其中並未包括釋字第 603 號解釋中所認定為敏感性個資之「指紋」。敏感性個資究為所指，仍有深究之必要。是故，本文第一個研究之問題是：「**何謂敏感性個人資料**？」本文以下將綜觀比較法上的發展與分類，並考慮近年來新興科技所引發的影響，[14]參酌我國國情與現行法規定後，[15]提出一套合理的定義方法。

二、敏感性個資是否得以蒐集、處理及利用？

在掌握敏感性個資之概念後，本文接續討論敏感性個資之蒐集、處理及利用。

---

[12] 英國資料保護法 §2

[13] 澳洲隱私法 §6

[14] 例如網際網路盛行已造成個人照片廣泛流傳，從個人照片上之特徵，通常得判斷出其種族，則蒐集、處理此類個人照片是否有違反「個資法」之虞，不無疑問。

[15] 例如是否增列「政治意見」；敏感性個人資料之特別規定，例如「醫療法」第 67 條至第 74 條有關病歷之規範。

由於揭露敏感性個資，將使個人遭受到不可彌補的傷害與誤會，進而對自由與隱私造成侵害。[16]原則上應禁止任何人蒐集、處理及利用敏感性個資，僅於符合法定例外情況時，得豁免限制而蒐集、處理及利用敏感性個資。[17]

所謂法定例外情況，我「個資法」規定四種得四種例外情形，分別為：

一、法律明文規定。

二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。

「歐盟個資指令」第 8 條第 2、3 及第 4 項規定數種例外情況，本文暫擬分為六類：

1. 涉及資料主體利益：資料主體(data subject)明示同意者；或為保護資料主體或第三人之重大利益，而資料主體無法表示同意者。[18]
2. 涉及資料控制人履行法定義務：資料保管人於僱傭法律關係中，為履行其法定義務或執行特定職權目的所必要者。[19]

---

[16] Directive 95/46/EC Recital 33 (“Whereas data which are capable by their nature of infringing *fundamental freedoms* or *privacy*…”) [emphasis added].

[17] 對於我國個資法所謂之「蒐集、處理及利用」,「歐盟個資指令」概以「處理」(process)一詞統稱之，參見本文第二章第一節之討論與 Directive 95/46/EC Art.2 (b)

[18] Directive 95/46/EC Art.8.2 (a) & (c)

3. 涉及特別種類非營利性組織內之會員事項：非營利組織於舉行合法活動時，就其會員或相關者所為之處理，且非屬未經當事人同意而向第三人為揭露者。[20]
4. 資料已為當事人自行公開或基於訴訟之必要者：該資料顯然已為資料主體所公開；或為成立、行使或防禦其法律上的主張所必要者。[21]
5. 涉及健康資料：為預防醫療(preventive medicine)、醫學診斷(medical diagnosis)與看護、治療或醫療服務管理之規定(provision of care, treatment or management of healthcare services)所要求者。[22]
6. 涉及重大公益：基於重大公共利益，且對該資料設有安全保護措施者。[23]

此外，「歐盟個資指令」尚就犯罪紀錄、保安處分與國民身份證號碼之使用規範，有原則性的規定。[24]敏感性個資僅符合上述情形時，得蒐集、處理及利用之，惟我「個資法」所規定之情況，與「歐盟個資指令」類別與數量有顯著之差異，我「個資法」之規定是否不足，殊值研究。綜上所述，本文研究的第二個問題：「**何時得蒐集、處理或利用敏感性個人資料？**」。本文將先討論我「個資法」規定之得失，並參酌各國立法例之規定，提出修正之建議。

三、蒐集、處理或利用敏感性個資所應遵循之「個人資料保護原則」，與一般個人資料有無不同？

資料控制人於蒐集、處理及利用敏感性個資時，**須遵守個人資料保護原則**。[25]

---

[19] Directive 95/46/EC Art.8.2 (b)

[20] Directive 95/46/EC Art.8.2 (d)

[21] Directive 95/46/EC Art.8.2 (e)

[22] Directive 95/46/EC Art.8.3

[23] Directive 95/46/EC Art.8.4

[24] Directive 95/46/EC Art.8.5 & 8.7

[25] 此即資料控制人應踐行之個人資料保護義務，參見 Deryck Beyleveld, *An Overview of Directive 95/46/EC in Relation to Medical Research, in* THE DATA PROTECTION DIRECTIVE AND MEDICAL RESEARCH ACROSS EUROPE 11 (Deryck Beyleveld et al. eds., 2004); ROSEMARY JAY & ANGUS HAMILTON, DATA PROTECTION: LAW AND PRACTICE 189-190 (2003).

所謂個人資料保護原則，一般泛指OECD「個人隱私與跨境個人資料流通保護綱領」（下稱「OECD 個資綱領」）[26]中之八大原則，包括「蒐集限制原則」(Collection Limitation Principle)、「資料品質原則」(Data Quality Principle) 等。[27]近年則以「歐盟個資指令」之「**資料品質原則**」與「**正當處理原則**」(Legitimate Processing Principle)等較為精簡。所謂「資料品質原則」規定在「歐盟個資指令」第 6 條，各會員國（亦即資料控制人）應當規定個人資料須：[28]

1. 合法且公平處理(processed fairly and lawfully)。
2. 蒐集資料之目的應特定(specified)、明確(explicit)、合法(legitimate)，且不得使用於與原始蒐集目的顯不相容(incompatible)之情形。
3. 蒐集、處理資料應適當(adequate)、相關(relevant)且不逾越原始目的(not excessive in relation to the purposes for which they are collected and/or further processed)。
4. 保持資料正確(accurate)、完整(complete)與更新(up-to-date)。
5. 以可得辨識資料主體之格式儲存資料者，其蒐集及處理不逾越原目的之必要期間(no longer than is necessary for purposes for which the date were collected or for which they are further processed)。

其中，第一項之「合法且公平處理」通常係指「正當處理原則」。該原則規定各會員國（亦即資料控制人）處理個人資料須符合六種情形之一：[29]

1. 當事人**明確同意**

[26] OECD Guidelines on the Protection of the Privacy and Transborder Flow of Personal Data § 7

[27] 此外尚有「目的明確原則」(Purpose Specification Principle)「使用限制原則」(Use Limitation Principle)、「安全保護原則」(Security Safeguards Principle)、「公開原則」(Openness Principle)、個人參與原則(Individual Participation Principle)與責任歸屬原則(Accountability Principle)。

[28] Directive 95/46/EC Art.6

[29] Directive 95/46/EC Art.7

2. 當事人為訂立**契約**所必須
3. 資料控制人為**履行法定義務**
4. 為保護當事人之**合法權益**
5. 為增進**公共利益**或為**執行法定職務**所必須
6. 為**維護第三人合法權益**，但不得損害當事人自由及人權

個人資料具備上述六種情形**之一**時，該資料可謂「正當」處理。惟上述個人資料保護原則類別複雜，先後次序也有所不同。這些原則面對敏感性個資時，是否有不同程度之放寬或限縮，值得研究。本文欲研究之第三個問題為：「**蒐集、處理或利用敏感性個人資料時，其須遵守之個人資料保護原則，在程度上與處理『非』敏感性個人資料有何區別**？」，本文將檢視公務機關或非公務機關，蒐集、處理或利用敏感性個資時，應適用之個人資料保護原則。

參、研究方法暨範圍

本研究主要採取文獻分析法，以我「個資法」作為研究基礎架構，參照「歐盟個資指令」與其他國家之個人資料保護法，例如同屬歐盟成員國之英國、德國，以及其他非屬歐盟成員國之國家，例如加拿大、澳洲。針對各國個人資料保護法(Data Protection Act)或隱私法(Privacy Act)中，有關敏感性個人資料保護之法制與爭議，進行比較與研究，最後參酌我國現行法之規定，提出可能之修正建議。

首先，本文將檢視我「個資法」定義之敏感性個資，並與各國立法進行比較討論，歸類出基本類型與定義方法，以供參考。次者，本文將針對「個資法」規定之四種豁免禁止，得蒐集、處理或利用敏感性個人資料之情形，逐次探討其適用上之疑義。最後，根據「OECD 個資綱領」與「歐盟個資指令」，本文擬定一套「個人資料保護原則」標準，將依照敏感性個資之「蒐集」、「處理」及「利用」

三階段，依次檢視敏感性個資適用「個人資料保護原則」之情形。

肆、研究架構

第一章為「緒論」，介紹本文研究背景與問題意識，說明研究目的與研究方法。第二章為「敏感性個人資料概念」，分為四節，首先就有關個人資料保護法之相關概念予以釐清，進而逐次討論敏感性個資之概念沿革與各國立法例，最後整理敏感性個資之界定方法。第三章為「敏感性個資之蒐集、處理及利用─原則禁止、例外許可」分為兩節，首先討論敏感性個資之禁止蒐集、處理及利用，進而討論豁免限制，得蒐集、處理或利用之例外情形。第四章為「敏感性個人資料保護原則」，根據個人資料之處理流程，即「蒐集」、「處理」及「利用」，逐次檢視公務機關或非公務機關（資料控制人）於蒐集、處理或利用敏感性個資時，所應遵循之個人資料保護原則。第五章提出研究發現與我國法之修正建議。

第二章　敏感性個人資料概念

本文旨在研究敏感性個人資料（下稱「敏感性個資」）之保護。為易於理解，茲擬先就「敏感性個人資料之概念」進行探索，並針對各國立法例，歸納出界定「敏感性個資」之方法，以供參考。由於「敏感性個資」屬於「個人資料保護法」之領域，討論「敏感性個資」所需要之用語概念，皆與「個人資料保護法」相關，以下先予釐清。

第一節　相關概念

一、個人資料

我「個資法」第 2 條定義：「個人資料」係指「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。「歐盟個資指令」第 2 條a款定義：「個人資料」(personal data)係指「**任何有關已識別或足資識別之自然人之資訊**」；[30] 所謂「足資識別之自然人」，係指其身份得藉由「身份辨識號碼」(identification number)或「其他相關因素」（例如生理、心理、精神、經濟、文化或社會身份），

[30] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of *individuals* with regard to the processing of personal data and on the free movement of such data Art.2(a) (“personal data” shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”). 中譯參照熊愛卿，《網際網路個人資料保護之研究》，國立台灣大學法律研究所博士論文，附錄（1999 年）。

得直接或間接確定者。[31]如上定義，尚有以下疑義：

1.「死者」之資料屬「個人資料」？

查「個資法」之前身「舊個資法」(84/08/11)對此未明確定義。根據法務部於2011年10月26日公告之「個人資料保護法施行細則」修正草案（下稱「個資法施行細則草案」)，第2條定義：「本法所稱個人，指**現生存之自然人**」，其修正理由謂：「本法立法目的之一為個人人格權之隱私權保護，唯生存之自然人方有**隱私權受侵害之恐懼情緒**及**個人對其個人資料之自主決定…**」，即認我「個資法」僅保護「現生存自然人」之資訊隱私權。

此外，查外國立法例，英國資料保護法(Data Protection Act 1998)定義：「個人資料」係指可得識別之「活人」(a living individual)的資料。澳洲隱私法(Australia Privacy Act 1988)定義：本法所稱之「個人」係指「自然人」(natural person)。澳洲「隱私官辦公室」(Office of the Privacy Commissioner)進一步認為，所謂「自然人」應限「活人」(living human)。[32]綜上所述，我「個資法」雖未明示「自然人」應排除「死者」，惟根據「個資法施行細則草案」與上開外國立法例，應可認為我「個

---

[31] *See id.* 已識別或足資識別自然人之「聲音」(sound)或「影像」(image)資訊仍屬「個人資料」，參見 Directive 95/46/EC Recital 14. 某些國家認為個資以聲音或影像方式儲存者，屬個人資料，例如葡萄牙、盧森堡及法國。*See* Douwe Korff, *EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws* 14 (Sep. 2002), *available at* http://www.garanteprivacy.it/garante/document?ID=455584

[32] 參見 1 AUSTRALIAN LAW REFORM COMMISSION, FOR YOUR INFORMATION: AUSTRALIAN PRIVACY LAW AND PRACTICE 8.65 & 355-84 (2008). 「澳洲法改會」(Australian Law Reform Commission, ALRC)建議，使用(use)或揭露(disclose)有關「死者」(deceased individuals)之個資，應符合隱私法之規定。資料控制人(data controller)使用或揭露「死者」之敏感性個資時，應注意資訊之「敏感性」(sensitivity of information)。

資法」所稱之「個人資料」，須為「現生存」自然人之資料，不及於「死者」。

2. 資料持有者「無能力識別特定個人」之資料，屬「個人資料」？

按我「個資法」第 2 條後段定義，「個人資料」須為得「以直接或間接方式識別特定個人」之資料。資料持有者（個人或組織）主觀上「無能力」(incapable)識別特定個人時，該資料是否仍屬「個資」，仍有疑義。

有關「個資」之概念，歐盟各國立法例率可分為兩類。第一，規定「個人資料」須為「得識別特定個人」之資料，無須考量資料持有者之識別能力或識別之方法；[33]第二，規定「個人資料」須為「資料持有者**有能力**識別特定個人」之資料。[34]

---

[33] 例如比利時，規定「以研究為目的」且「可充分辨識」(fully identifiable)、「編碼化」(encoded or pseudonymised)或「完全匿名化」(fully anonymised)之資料，屬於「個資」，無論資料持有者是否有能力識別特定個人。其他採取類似立場之國家例如丹麥、芬蘭、法國、義大利、西班牙與瑞典。此定義可避免掛一漏萬，保護範圍較廣。多數國家並參酌「資料之性質」(nature of data)來判斷「資料主體被識別的可能性」(probability of the data subject being identified)。相關討論參見 Korff, *supra* note 31, at 14-16.

[34] 採取類似立場之國家，例如奧地利、德國、荷蘭與英國，參見前註。此定義可避免擴大資料控制人之義務。有學者認為，經匿名化(anonymising)之資訊因無法識別特定個人（資料主體），故不能視為「個人資料」，參見 Carlos María Romeo Casabona, *Anonymization and Pseudonymization: The Legal Framework at a European Level*, *in* THE DATA PROTECTION DIRECTIVE AND MEDICAL RESEARCH ACROSS EUROPE 36, 42 (Dreryck Beyleveld et al. eds., 2004); PHILIP COPPEL, INFORMATION RIGHTS 5-025 (2007). 此外，匿名化與假名化(psedonymous)並不相同，資料經完全匿名化後，將無法回溯辨識當事人，故不屬於個人資料，而假名化後，得藉由資料控制人掌握之關鍵(key)回溯辨識當事人，仍受到個資法之保護，參見 CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 2.08-2.10 (2007).
值得注意者，英國法雖認為資料控制人有能力識別特定個人之資料，即屬「個資」，但英國法院在審理相關案件時，卻限縮上開定義。英格蘭及威爾斯上訴法院(England and Wales Court of Appeal)在 Durant v. Financial Services Authority 案([2003] EWCA Civ 1746, Court of Appeal (Eng.))

我「個資法」僅規定「得以直接或間接方式識別特定個人」之資料，為「個資」，似屬前開第一類情形，惟「個資法施行細則草案」第 3 條但書規定，「以間接方式識別」[35]且「查詢困難、需耗費過鉅或耗時過久始能識別特定個人」者，不屬「個資」，係考量資料持有者，因「能力（辨識技術或辨識效率）不足」，而無法間接識別特定個人，故將「資料持有者**無能力間接識別特定個人**」之資料排除「個資」概念之外，實與前開各國立法例第二類情形相同。

綜上，依我「個資法」與「個資法施行細則草案」之規定，資料持有者（公務機關或非公務機關）「得以直接或間接方式識別特定個人」之資料，原則上仍屬「個資」，惟資料持有者係以「間接方式」識別特定個人，且「查詢困難、需耗費過鉅或耗時過久始能識別特定個人」者，該資料將不屬「個資」。

3. 「統計資料」屬「個資」？

我「個資法」第 2 條定義：「個人資料」係指得以直接或間接方式識別該「自然人」之資料。記載多數自然人之「統計資料」(statistical data)，例如郵遞區號或各類意見調查，如可以從「統計資料」中識別「特定個人」，該「統計資料」即

認為，上訴人申請之「電腦化文件—尚未經編修之版本」(unredacted versions of the computerised documents)與「手寫文件」(manual records)不屬於「個人資料」。法院認為，僅憑被上訴人（資料控制人）之資料中記載上訴人，尚不能構成上訴人（資料主體）之個人資料，猶須：1. 有關資料主體之記載具有「連續相關性」(continuum of relevance)，亦即該記載須為「傳記性」(biographical)之記載；或 2. 得自與資料主體相關之事務中予以識別資料主體，亦即資料記載之「焦點」(focus)為資料主體，而非他人。

[35] 所謂「間接方式識別」，依「個資法施行細則草案」第 3 條，指僅以該資料不能[直接]識別特定個人，須與其他資料對照、組合、連結等，始能識別該特定個人者。

屬「個資」。[36]如僅能識別「一群（個）人」(a group of individuals)，則不屬「個資」。

二、（資料之）蒐集、處理及利用

我「個資法」第 2 條將個人資料之「操作」(operations)，分為三個流程，依序為資料之「蒐集」、「處理」及「利用」。[37]蒐集：「指以**任何方式取得**個人資料」；[38]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**」；[39]「利用」：「指將蒐集之個人資料為**處理以外之使用**」。[40]

有關個人資料之「操作」(operations)，各國立法例規範不一，有分為三個流程「蒐集」(collection)、「處理」(processing)及「使用」(use)者，例如德國聯邦資料保護法；[41]有分為「蒐集」(collection)、「使用」(use)與「揭露」(disclosure)，例如澳洲隱私法。[42]有以「處理」(processing)統稱所有資料之「操作」者，例如「歐盟個資指令」與英國資料保護法。[43]本文為求用語精確且符合「個資法」之規範，下

---

[36] 一般而言，單純的街景照片通常不會構成個人資料，但有系統蒐集照片再與個人連結，就會變成個人資料。荷蘭主管機關便認為某公司有系統的蒐集德國街區 360 度數位照片，假如會影響到個人時，該照片將構成「個資」，例如以此作為課稅依據，參見 Korff, *supra* note 31, at 16.

[37] 此概念早年係直接受德國聯邦資料保護法(Bundesdatenschutzgesetz, BDSG)之影響。

[38] 「個資法」第 2 條第 3 款。

[39] 「個資法」第 2 條第 4 款。

[40] 「個資法」第 2 條第 5 款。

[41] 參見德國聯邦資料保護法 §§ 3(3)(4) & (5).

[42] 參見澳洲隱私法附表三「國家隱私原則」(Npps)第 1 點與第 2 點。

[43] 參見英國資料保護法 § 1(1)；「歐盟個資指令」第 2 條規定，「個人資料處理」係指對個人資料所進行之任何或一系列操作，無論其是否以自動化方法進行，例如蒐集(collection)、記錄(recording)、組織(organization)、儲存(storage)、改編或修改(adaptation or alteration)、回復(retrieval)、參閱(consultation)、使用(use)、以傳輸或散佈而揭露(disclosure)或以其他使其有效的結合(alignment)或排列(combination)、封鎖(blocking)、消除(erasure)與破壞(destruction)。其他各國之

文概以「蒐集、處理或利用」統稱「個資」之「操作」。

三、資料控制人

各國個資法為徹底落實「個人資料之保護義務」，[44]率皆定義「保護義務」主體—「資料控制人」(data controller)之概念。[45]「資料控制人」係指：決定 [46]資料處理(processing)之「目的」(purposes)與「方法」(manner)之自然人或機構組織。

我「個資法」自「舊個資法」時期即未採用「資料控制人」之用語，而仿效德國、奧地利以「公務機關」與「非公務機關」，[47]作為「資料控制人」。現「個資

規定不及討論，參見湯德宗，〈電腦處理個人資料保護法 2008 修正草案評釋〉，發表於台灣法學會 2008 年年度法學會議（2008 年 12 月 20 日）。

[44] *See* KUNER, *supra* note 34, at 2.20 & 2.25; UK Information Commissioner, *DPA: Legal Guidance*, para. 2.5., *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

[45] 例如 Directive 95/46/EC Art. 2(d) & (e); 英國資料保護法 §1(1).
「資料控制人」概念下尚有「資料處理人」(data processor)，指「代表」資料控制人處理資料之自然人或組織，其係直接聽從資料控制人之命令而進行資料之操作。各國立法例對資料處理人之規定亦不相同，英國與愛爾蘭規定「受雇人」不得為資料處理人，德國並未直接定義資料處理人，法國則將資料處理人視為「收受者」(recipient)以外之人，參見 *See* Korff, *supra* note 31, at 23-24. 資料「收受者」之概念與「資料處理人」概念顯不相同，為避免資料控制人規避法律責任與義務，部分國家並未免規範「資料處理人」，而將處理者一律視為「資料控制人」。

[46] 在「歐盟個資指令」之架構下，尚須判斷「資料控制人」係「單獨或共同」(alone or jointly)作成決定，蓋「歐盟個資指令」假設「資料控制人」都是一個實體，遇到多重實體時，其責任之歸屬會產生適用上困難，此時須視各實體之資料庫間是否有「內部連結」(interconnected)與「共享」(shared)，此一「共享」概念與「某團體為了他方利益而向其提供資訊」顯然有別，參見 Korff, *supra* note 31, at 22-23.

[47] 參見德國聯邦資料保護法(Bundesdatenschutzgesetz, BDSG)第 2 條；奧地利聯邦個人資料保護法(Datenschutzgesetz 2000, DSG)第 5 條。

法」規定與「舊個資法」相同，「個資法」第 2 條定義：「七、公務機關：指依法行使公權力之中央或地方機關或行政法人；八、非公務機關：指前款以外之自然人、法人或其他團體」，意義上等於「資料控制人」。此外，「個資法」第 4 條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關」。受委託之機關無論其地位，於受委託執行「蒐集、處理或利用」個人資料時，仍該當「資料保護義務」之主體。故，公務機關、非公務機關或受委託機關，於進行個人資料之「蒐集、處理或利用」時，皆應遵守「個資法」之規範，履行「資料保護義務」。為行文方便，下文以「資料控制人」統稱「公務機關」與「非公務機關」。

第二節　敏感性個人資料概念之發展

1970年代起，拜資訊傳播科技(Information, Communication Technology, ICT)快速發展之賜，私人企業開始廣泛使用個人資料，致個人資料遭到誤用之風險日益升高。[48]1968年，經濟合作暨發展組織(Organization for Economic Co-operation and Development, OECD)乃針對當時之「科技缺口」(Gaps in Technology)召開部長級會議(Ministerial Meeting)，商討對策。[49]為避免個人資料於進行儲存、傳送、修改與處理時遭到誤用，而侵害個人利益，各國開始制定相關法規。[50]1970年，德國黑森邦(Land of Hesse)制定資料保護法(Datenschutzgesetz)[51]，堪稱今世第一部個人資料保護法，時僅適用於公部門。[52]同時期其他較具代表性之立法，例如瑞典資料法[53]、美國隱私法[54]與德國聯邦資料保護法[55]。

---

[48] *See* Neil Robinson et al., Technical Report, Review of the European Data Protection Directive, at 6, *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf (2009).

[49] *See* Hans Peter Gassmann, Former Head of the ICCP Division Directorate for Science, *Technology and Industrtry, OECD 30 Years After: The Impact of The OECD Privacy Guidelines*, Address at Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and its Working Party on Information Security and Privacy (WPISP) (Mar. 10, 2010), *available at* http://www.oecd.org/document/39/0,3746,en_2649_34255_44946983_1_1_1_1,00.html

[50] *See* David P. Farnsworth, *Data Privacy or Data Protection and Transborder or Transnational Data Flow, an American's View of European Legislation*, 11(4) INT'L BUS. LAW. 114, 114 (1983).

[51] Data Protection Act 1970 (Hessisches Datenschutzgesetz). *See* Godfrey Stadlen, *Survey of National Data Protection Legislation*, 3(3) COMPUTER NETWORKS 174-186 (1976); Frits W. Hondius, *Data Law in Europe*, 16 STAN. J. INT'L L. 87, 92 n.10 (1980); ROBERTO J. RODRIGUES ET AL., THE REGULATION OF PRIVACY AND DATA PROTECTION IN THE USE OF ELECTRONIC HEALTH INFORMATION 76 (2001).

[52] *See* Gassmann, *supra* note 49.

[53] Data Law 1973. 北歐之個資法發展可參見 Lee A. Bygrave, *Data Protection Reform in Scandinavia*, 5 PRIVACY L. & POL'Y REP. 9-12 (1998).

[54] U.S. PA 5 U.S.C. § 552a.

[55] Germany Bundesdatenschutzgesetz, BDSG.

有關敏感性資料(sensitive data)之概念，曾出現在上開德國黑森邦之資料保護法與瑞典資料法中，[56]但其年代久遠，文獻多未見詳細討論。多數研究乃以1980年起的數個主要國際公約作為其概念之濫觴，[57]茲分述如下。

一、OECD 個資綱領

1980年，經濟合作暨發展組織為保護隱私與個人自由，擬訂「個人隱私與跨境個人資料流通保護綱領」（Annex to the Recommendation of the Council of 23rd September 1980: GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, 下稱「OECD個資綱領」）。「OECD個資綱領」其最初草案曾定義「敏感性個資」之概念，嗣專家小組(Expert Group)就敏感性個資之認定標準（例如差別待遇的風險(the risk of discrimination)）進行討論後，認為「無法定義普世(universally)的敏感性個人資料」，乃刪除草案之定義，故後來通過之「OECD個資綱領」中並未明確定義「敏感性個資」。[58]此外，有關「敏感性個資」之概念，在「OECD個資綱領」B部分細部評論(detailed comments)第七段「合法蒐集原則」中有如下記載：[59]

---

[56] *See* Spiros Simitis, *Revisiting Sensitive Data*, Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, at 1, *available at* http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Simitis_1999.pdf; Karen McCullagh, *Data Sensitivity: Proposals for Resolving the Conundrum*, 2 J. INT'L COM. L. & TECH. 190 (2007).

[57] *See* McCullagh, *supra* note 56; Rebecca Wong, *Date Protection Online: Alternative Approaches to Sensitive Data*, 2(1) J. INT'L COM. L. & TECH. 9 (2007). The developments of the data protection in European before the 1980's conventions, *see generally* A. C. Evans, *European Data Protection Law*, 29 AM. J. COMP. L. 571 (1981).

[58] OECD Guidelines on the Protection of the Privacy and Transborder Flow of Personal Data, Part I, para.19 & Part II B. Detailed Comments, para.50.

[59] OECD Guidelines on the Protection of the Privacy and Transborder Flow of Personal Data, Part II B. Detailed Comments, para.50.

「第七段討論兩個議題。亦即，(a) **限制資料之蒐集**(limits to the collection of data)，**因為資料處理之方式**(manner)、**資料之特性**(nature)**與利用該資料之情境**(context)**或其他情形，該資料被視為特別敏感**(specially sensitive)。(b) 有關資料蒐集方法之規定(requirements concerning data collection methods)。關於第一個問題，常有不同意見。有人主張定義**敏感性資料類別是可能且符合期望的，且該資料之蒐集必須加以限制甚或完全禁止**，部分歐洲國家已存有立法先例（例如種族、宗教信仰、刑事紀錄等資料）。另一方面，有人則主張或許**所有的資料，本質上都不具私人性或敏感性，只有在資料處於特定的情境**(context)**或使用**(use)**時，始具備『隱私』**(private)**或『敏感性』**(sensitive)。[60]這樣的觀點反應於，例如美國的隱私立法[61]」。

前揭評論對於應否定義「敏感性個資」一事，提出兩種截然不同的觀點。第一種是直接定義敏感性個資，並將**敏感性個資之概念與「蒐集限制原則」**(Collection Limitation Principle)**連結**，[62]認為應禁止蒐集「特別敏感」(specially sensitive)之個資；第二種則**將資料視為中性，須依其情境予以判斷是否得予以蒐集、處理之**。第一種見解比較直觀，無須判斷資料使用之情形，只要該資料顯示或記載之資訊，符合表列種類，即加以限制，此見解影響各國立法，堪稱目前通說。第二種見解稍微複雜，它先將所有資料定性為「中性」（或無害），僅於該資料被蒐集或處理

[60] 此見解與釋字 603 號余雪明大法官「部分協同、部分不同意見書」類似（指紋僅為「中性之身分辨識工具」，且不能因指紋所聯結之資訊本身敏感，而認為指紋亦為敏感性個資。所應禁止或限制者為該項敏感資訊之蒐集，而非指紋或姓名）。

[61] 蓋美國法並無統一的敏感性個資定義，而係根據資料處理或使用之性質，分屬不同法規規範，詳見下節討論。

[62] 「OECD 綱領」第 7 條規定，個人資料之蒐集應有限制，且僅得以合法且公平之方法獲得，並通知資料主體或經資料主體之同意。

時，才可能對個人隱私造成侵害。該見解常成為反對定義敏感性個資的主要理論。[63] 雖然「OECD個資綱領」對於OECD各會員國未具有強制性，但該規定仍影響包括歐盟成員國或是澳洲、紐西蘭、香港以及我國之個人資料保護法。[64]

二、歐盟「保護個人關於自動化處理個人資料公約」

1981 年，歐洲理事會(the Council of the European Union)[65]為保護經自動化處理之個人資料，發佈「保護個人關於自動化處理個人資料公約」(Convention For The Protection of Individuals With Regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, 下稱「歐盟個資公約」)。「歐盟個資公約」為第一個定義敏感性個資之國際公約，第 6 條規定：除國內法已提供適當的安全措施者外，[各締約國]不得對顯示下列內容之個人資料，進行自動化處理：**種族、政治主張、宗教或其他信仰**[66]，以及與**健康、性生活與刑事判決有關**之個人資料。[67]「歐盟個資公約」採用前述「OECD個資綱領」的第一種見解，即直接以「資料顯示或

---

[63] 參見本章第四節。

[64] *See* McCullagh, *supra* note 56, at 190.

[65] 歐盟理事會之主要職權在於向各會員國匯報並作成政治決策。理事會在兩件事情上影響資料保護。第一，提供各會員國於行使立法權時之政治討論空間；其次，透過「歐盟個資指令」第 31 條的委員會。理事會同時也建立「工作小組」(working party)來處理資料保護事項。相關討論參見 KUNER, *supra* note 34, at 1.11 & 1.12.

[66] 根據「歐盟個資公約」的「解釋報告」(Explanatory Report)，表達政治意見、宗教或其他信念之活動(activities)屬「敏感性個資」，參見 Directorate General of Human Rights and Legal Affairs, *Data Protection: Compilation of Council of Europe texts*, para.44, *available at* http://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf

[67] Convention for The Protection of Individuals with Regard to Automatic Processing of Personal Data Art. 6 [*hereinafter* Convention 108] "Personal data revealing *racial origin, political opinions or religious or other beliefs*, as well as personal data concerning *health or sexual life*, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to *criminal convictions*." (emphasis added).

記載之內容」定義敏感性個資，並禁止各締約國[68]將該種個資進行自動化處理，除非各國已提供適當保護措施者外。[69]

用語概念上，「歐盟個資公約」並未使用「敏感性資料」(sensitive data)一詞，而係以「特種資料」(special categories of data)稱之。但無論哪一種用語，所指涉的皆為同一概念。另一方面，「歐盟個資公約」第 6 條所指稱之「自動化處理」(processed automatically)與前述「OECD個資綱領」所提之「資料蒐集」(collection of data)，兩者之概念意涵實質上並不相同。蓋根據「歐盟個資公約」第 2 條C款之定義：「自動化處理」(processed automatically)係包含以自動化方法，全部或部分地儲存數據，以進行邏輯或數學運算，修改、刪除、回復或散佈資料。[70]「歐盟個資公約」所規範者屬資料持有人「取得資料後」所進行之「操作」行為，例如我「個資法」定義之「處理」及「利用」，而不包括「取得資料前」之操作行為，例如「蒐集」或「取得」資料。「OECD個資綱領」則建議「直接限制蒐集」，與「歐盟個資公約」有所不同。

---

[68] 該公約原先僅開放歐洲理事會成員國簽署，其他國家須待一定條件下（第 23 條）始能簽署本公約，故公約最後之簽署國家，並不限於當時歐洲共同體成員國，公約之名稱「歐洲」或可當作形容詞理解，參見 Colin Tapper, *New European Direction in Data Protection*, 3(1) J.L. & INFO. SCI. 9, 12 (1992).

[69] 該公約規定各締約國得根據下列理由，另訂處理特種資料之情形：維護國家安全、公共安全、國家財政利益或遏止犯罪；保護資料主體或他人之權利或自由，參見 Convention 108 Art. 9(2) ("Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. *protecting State security, public safety, the monetary interests of the State* or *the suppression of criminal offences*;

b. *protecting the data subject* or *the rights and freedoms of others*") (emphasis added).

[70] Convention 108 Art.2(b) ("automatic processing" includes the following operations if carried out in whole or in part by automated means: *storage* of data, carrying out of *logical and/or arithmetical operations* on those data, their *alteration, erasure, retrieval* or *dissemination*) (emphasis added).

「歐盟個資公約」為國際條約中首次清楚明確定義敏感性個資，[71]藉此與其他個人資料加以區別，各會員國並應當透過其國內法採取必要措施。[72]「歐盟個資公約」的「解釋報告」(Explanatory Report)[73]部分同意前述「OECD個資綱領」的第二種見解（將資料皆視為中性，資料僅於特定「情境」(context)才會對個人隱私造成侵害），「解釋報告」認為：通常情況下，**「資料之內容(contents)」並不會對個人造成傷害，只有「資料之使用情境(context)」才會對個人造成傷害，但某些特殊類型資料，其「資料之內容」卻很可能侵害個人權利與利益**。「解釋報告」進一步指出，「歐盟個資公約」所規定之「特種資料」，通常在各會員國內已被認為係「特別敏感」(especially sensitive)。[74]至於其「敏感度」(degree of sensitivity)，則須取決於各國的法律與社會環境(legal and sociological context)。[75]

從字面上觀察，吾人或許會以為前述這兩種概念為相斥關係，但若基於保護個人資訊隱私與個人資訊自決權之目的，**本文認為應可將第一種見解（敏感性個**

---

[71] *See* McCullagh, *supra* note 56, at 191.

[72] Convention 108 Art.4

[73] Directorate General of Human Rights and Legal Affairs, *Data Protection: Compilation of Council of Europe texts, available at* http://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf

[74] *See id*. para. 43

[75] *See id*. para. 48. 「解釋報告」同時認為：公約所列舉之敏感性個資僅為例示規定，各簽約國仍得根據公約第 11 條之延伸保護條款，增定其他類別之資料為敏感性個資，例如工會會員資料。惟近年來，隨著科技持續發展，資料之形式與種類不斷擴張。歐盟針對「歐盟個資公約」之研究報告遂建議新增「識別號碼」(identification number)與「生物辨識資訊」(biological and biometric data)為敏感性個資，參見 Jean-Marc Dinant, Cécile de Terwangne & Jean-Philippe Moiny, Report on the lacunae of the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No 108) resulting from technological developments T-PD-BUR(2010)09 E, at 9, *available at* http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD-BUR_2010_09_en.pdf

資之「內容」(content)易侵害個人隱私與權利）視為主要解釋，而將第二種見解「資料僅於特定情境(context)下，始具備敏感性」視為輔助性解釋。立法者應先依第一種見解，根據資料之「內容」定義敏感性個資；再依照各國社會環境與資料蒐集、處理或利用之「情境」，擴張或限縮敏感性個資之定義，方為周詳。

最後，由於「歐盟個資公約」僅規定締約國應以「國內法採取必要措施」[76]來實現該公約之內容，未強制要求締約國「立法」保護個人資料，[77]因此使各國個人資料保護水平差異過大，[78]是故「歐盟個資公約」並未如期成功提升個人資料之保護。[79]

三、聯合國「規範電腦化個人資料檔案指導綱要」

1990年，聯合國發佈「規範電腦化個人資料檔案指導綱要」(Guidelines for the Regulation of Computerized Personal Data Files, 下稱「個資規範」)[80]。「個資綱要」捨棄前述「敏感性」或「特種」資料之用語。「個資規範」第五點「非歧視原則」(Principle of non-discrimination)揭示：資料會造成「非法的」(unlawful)或「恣意的」(arbitrary)歧視(discrimination)時，應不予處理，包括**種族、膚色、性生活、政治主**

---

[76] 「必要措施」包括得自由選擇以「立法」或「發佈命令」訂之，*See id*. para 46.

[77] Convention 108 Art.4(1). ("Each Party shall take the *necessary measures* in its domestic law to give effect to the basic principles for data protection set out in this chapter") (emphasis added).

[78] 例如當時英國個資法排除保護人工資料，而德國黑森邦之個資法卻包括人工資料。同時，英國建立起詳細的登記系統制度，其他國家卻無，參見 McCullagh, *supra* note 56, at 191; Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 478 (1994-1995); Evans, *supra* note 57, at 579.

[79] *See id*. 2011 年 1 月，歐盟執委會與理事會於布魯塞爾召開會議以紀念該公約簽訂 30 週年。理事會於會中提議修正本公約以符合科技發展與國際化標準，詳細討論參見 Julia de Oliveira, *EU Directive and CoE Convention are being revised in parallel*, 109 PRIVACY L. & BUS. INT'L REP. 23 (2011).

[80] G.A. res. 44/132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989).

張、宗教、哲學及其他信仰，與社團或工會成員的資料[81]。「個資規範」對於敏感性個資的定義較前揭「歐盟個資公約」廣泛，它增加「膚色」(colour)、「工會或社團成員」(membership of an association or trade union)，然而卻不包括「刑事判決」(criminal convictions)與「健康資料」(health data)，此番差異，顯示出國際上仍缺乏統一的敏感性個資定義。

四、歐盟「個人資料保護指令」

（一）背景與目的

二次戰後，包含「聯合國人權公約」(Universal Declaration of Human Rights, UDHR)[82]、「歐洲人權公約」（The Convention for the Protection of Human Rights and Fundamental Freedoms, ECHR）[83]與「聯合國公民與政治權利公約」(International Covenant on Civil and Political Rights, ICCPR) [84]皆將「隱私」(privacy)視為一種基本人權，作為隱私概念底下之「個人資訊隱私權」或「個人資訊自主決定權」，亦即個人資料之保護，同樣受到國際間的重視。

由於前述「歐盟個資公約」未強制締約國須立法制定「資料保護法」或訂定任何限制，[85]致使歐盟會員國內之個人資料保護水平不一，連帶阻礙各會員國間之

---

[81] Guidelines for the Regulation of Computerized Personal Data Files, Principle 5 ("Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on *racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs* as well as *membership of an association or trade union*, should not be compiled") (emphasis added).

[82] G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948). Art. 12

[83] OG A 256, LD 53/1974 Art. 8

[84] ICCPR Art. 17

[85] *See* Simitis, *supra* note 56, at 2.

資料流動，形成發展內部市場之障礙。[86]為了確保資訊自由流動與個人資料保護，1995 年歐盟執委會(European Commission)[87]，向歐洲議會(European Parliament)[88]及理事會提出「個人資料保護指令」(Directive 95/46/EC)。[89]

「歐盟個資指令」的規範對象是「個人資料」(personal data)，而非廣泛的「隱私」。「歐盟個資指令」的主要目的在建立制度性框架、協調成員國相關法律規定，以保護資料主體（本人）之資訊隱私權，並創造資訊自由流通的單一歐洲市場。[90]

---

[86] 此即所謂 first pillar，根據歐體條約第 7a 條規定，應當確保貨物、人員、服務和資金在歐盟內部市場內自由流動，參見「歐盟個資指令」前言第 3 點。

[87] OJ No C 277, 5. 11. 1990, p. 3 & OJ 311, 27. 11. 1992, p 30.
歐盟執委會為歐盟之行政機關，底下分為 38 個 Directorates General(DGs)，其中 DG Justice, Freedom and Security(DG JLS)處理資料保護事項，並對 DG Information Society(DG INFSO)負責，其他的機構僅於面臨特殊領域的個資爭議時，才會處理資料保護議題，例如 DG Employment and Affair 負責勞工之資料處理。此外，執委會並不負責執行歐盟指令規範的事情，這部分僅交由各國單方自行實施，唯一具有法律拘束力之機關為歐洲法院(European Court of Justice, ECJ)。此外，歐洲資料保護機構(European Data Protection Supervisor, EDPS)負責監管歐盟機關之個人資料處理，其為一獨立監管機關，並獨立於政治影響力外，但它能實質影響歐盟層級的資料保護政策制定。它擁有權力可以干涉任何尚未進入 ECJ 的資料保護案件，它對於執委會的政策制定相當重要。相關討論可參見 KUNER, *supra* note 34, at 1.09, 1.10, 1.16 & 1.17

[88] 歐洲議會在歐盟資料保護立法中，扮演重要角色。議會中的部分委員會負責處理資料保護爭議，例如境內市場與顧客委員會(internal market and consumer)或法律爭議委員會(legal affairs)、公民自由正義與家庭事務委員會(civil liberties, justice and home affairs)。歐洲法院(European Court of Justice)擁有個資法的最終裁決權。它透過兩方面來處理個資爭議。第一，會員國或執委會可向法院提起訴訟；其次，由會員國法院呈請歐洲法院提供個資法之解釋意見。相關討論參見 KUNER, *supra* note 34, at 1.13 & 1.14

[89] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050. 有關「歐盟個資指令」草稿之評釋，可參見 Joseph I. Rosenbaum, *The European Commission's Draft Directive on Data Protection*, 33 JURIMETRICS J. 1 (1992-1993).

[90] *See id*. 相關目的可參閱「歐盟個資指令」前言序言第 7 點（鑑於各成員國於個人資料處理時，

「歐盟個資指令」序言(Recital)第10點謂：由於各國個人資料保護法係為保護基本權利與自由，特別是「歐洲人權公約」與共同體基本法律原則所承認之隱私權，故各國應確保歐洲共同體內之個人資料保護水平。[91]「歐盟個資指令」第1條第1項宣示：「為與本指令相符，會員國應保護自然人之基本權利與自由，特別是關於處理個人資料之隱私權」。[92]「歐盟個資指令」所欲保護之基本權利與自由（隱私），同樣也受到ECHR的明文保護，進而構成共同體法律之基本原則，並具「優越、憲法重要性」(overriding, constitutional importance within the legal order of the Community)。2000年歐盟簽署的「歐盟基本權利憲章」(Charter of Fundamental Rights of the European Union)第8條即清楚揭示「個人資料保護權利」[93]。

對個人權利與自由，特別是隱私權所提供之保護水平不一，會阻止資料之跨國傳輸；鑑於此差異將形成共同體經濟活動之障礙…）、第 8 點（為了消除個人資訊流動的障礙，各成員國於涉及個人資料處理時，其保護個人權利與自由之水平應維持相同標準…）與第 9 點（鑑於各國採取相同保護標準，各成員國不得以保護個人權利與自由為由，限制個人資料之自由流動…）。

[91] Directive 95/46/EC Recital 10 "... the object of the national laws on the processing of personal data is *to protect fundamental rights and freedoms, notably the right to privacy*, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law." (emphasis added).

現況上，歐盟法下之個人基本權利保護，略可回溯自三種不同的根源。第一，基於「歐洲人權公約」之普遍原則與各會員國之憲法傳統；第二，「歐盟基本權利憲章」（Charter of Fundamental Rights of the European Union, 下稱「憲章」）所規定應予保護者；第三，歐盟加入 ECHR 後應進行保護之權利，參見 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, OJ C 306, 17 December 2007 Art. 6; Privacy International, *European Union-Privacy Profile*, https://www.privacyinternational.org/article/european-union-privacy-profile#contents (last visited Dec. 30, 2011).

[92] Directive 95/46/EC Art. 1(1) "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, *and in particular their right to privacy with respect to the processing of personal data*." (emphasis added).

[93] Art. 8 該憲章同樣確認了「表意自由」(right to freedom of expression)，參見憲章第 11 條與 ECHR 第 10 條

一般認為，「歐盟個資指令」序言第10點清楚承認「資料保護」的憲法地位。[94]惟「個人資料保護」之權利是否皆受到歐盟各國憲法保護，或僅存在於法律規範位階，卻存在明顯差異。目前僅有荷蘭、葡萄牙與西班牙明確於憲法中規定個人「資料保護」權利，規範方式類似「歐盟基本權利憲章」第8條，將「個人資料保護權利」視為一項單獨的權利(sui generis right)。[95]其他國家則未明文規定，[96]或與不同的權利概念結合。[97]總之，各國之「資料保護」植基於不同範圍的「憲法原則與權利」(constitutional principles and rights)上，[98]即便「資料保護」源自類似的原則，但其未必具有相同的原理，例如德國聯邦憲法法院自「人格權」中發展「資訊自決」(information self-determination)原則；法國「國家資訊自由委員會」(The Commission nationale de l'informatique et des libertés, CNIL)認為「拒絕權」(right to object)則是「資訊自決概念最明白且清楚的體現」。荷蘭最高法院則認為「資料保護」係「一般人格權」(general personality right)。[99]

（二）指令之規範

「歐盟個資指令」仿效「歐盟個資公約」以「特種資料」(Special categories of

---

[94] *See* Korff, *supra* note 31, at 7.

[95] *See id*. at 8.

[96] 德國即藉由「人格權」(general right to respect for one's personality, das allgemeine Persönlichkeitsrecht)來保護個人資料。法國則基於憲法對於「人性尊嚴」(human identity)、「人權、私人生活與個人、公眾自由」(human rights, private life and individual and public liberties)的尊重。

[97] 例如比利時、盧森堡與「隱私」；芬蘭則與「私人生活與榮譽」(private life and honour)；義大利與「隱私與個人尊嚴」(privacy and personal identity)；希臘與「私生活、人性尊嚴與價值」(private life, human dignity and–value)；瑞典則與「人格健全」(personal integrity)連結。至於芬蘭則與「隱私權」相連，惟其「隱私權」係為未明文列舉之憲法權利。

[98] *See* Korff, *supra* note 31, at 9.

[99] 相關討論參見 Korff, *supra* note 31, at 8-10.

data)稱呼「敏感性個資」。「歐盟個資指令」第 8 條第 1 項規定：[100]

「凡**顯示種族血緣、政治意向、宗教或哲學信仰、工會會員資格之個人資料**及**涉及個人醫療或性生活**等資料，會員國皆**不得處理**之」。

第 5 項就刑事記錄為特別之規定：[101]

「關於**犯罪、刑事判決或保安處分等資料**之處理，須由公務機關監管，或國家法律已提供適當特定之安全維護措施者，會員國得訂定例外條款。刑案**有罪判決之完整紀錄**，應限由公務機關監管」。[102]

---

[100] Directive 95/46/EC Art.8.1 "Member States shall prohibit the processing of personal data revealing *racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership,* and the processing of data *concerning health or sex life*." (emphasis added).

[101] Directive 95/46/EC Art.8.5 "Processing of data relating to *offences, criminal convictions* or *security measures* may be carried out only under the control of official authority, or if *suitable specific safeguards* are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority." (emphasis added).

[102] 2012 年「歐盟執委會」(European Commission)提出「個人刑事資料保護指令」草案(Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data)，以規範各國主管機關(competent authorities)處理有關「刑事犯罪之預防、調查、偵察與起訴」(prevention, investigation, detection or prosecution of criminal offences)與「刑罰之執行」(the execution of criminal penalties)之個人資料，參見 Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data COM(2012) 10 final.

第 7 項規定：會員國應制定**國民身份號碼**(national identification number)或其他**通用識別號碼**(identifier of general application)之處理規定。

「歐盟個資指令」與「OECD個資綱領」相比：「歐盟個資指令」清楚定義敏感性個資，「OECD個資綱領」未定義敏感性個資；「歐盟個資指令」與「歐盟個資公約」相比：「歐盟個資指令」定義之敏感性個資是列舉規定，「歐盟個資公約」定義之敏感性個資的類別只是例示規定。[103]「歐盟個資指令」與「UN個資綱要」相比，「歐盟個資指令」之定義不包含「膚色」、「社團成員」，但卻對「刑事判決」有特殊規定。惟此分類並非全然不受批評，[104]在奧地利、芬蘭、瑞典與英國共同提出的「資料保護指令修正提案」(Data Protection Directive (95/46/EC) Proposals for Amendment made by Austria, Finland, Sweden and the United Kingdom, 以下稱「歐盟個資指令修正案」) 中，[105]便認為「歐盟個資指令」之定義過於模糊。資料主體（本人）除非是戴面具或是易容，否則公開其照片也可以被認為是揭露其種族血緣資料，[106]故建議參酌「歐盟個資指令」序言第 33 點，認為資料本身難以避免附帶顯示(incidental revelations of the characteristics)諸如「種族血緣」或「宗教或哲學信仰」等敏感性個資之特徵者，該資料不屬敏感性個資，以避免過度擴張敏感性個資之定義。[107]值得注意者，有關敏感性個資之性質，「歐盟個資指令」序言第 33 點認為：敏感性個資之性質可能對個人之自由和隱私造成侵害，「歐盟個資指令修正案」

---

[103] *See* McCullagh, *supra* note 56, at 192; Simitis, *supra* note 56, at 3.

[104] 一位冰島的受訪者認為他們並不在乎工作地點與所屬工會的問題。相關討論參見 McCullagh, *supra* note 56, at 193.

[105] Data Protection Directive (95/46/EC) Proposals for Amendment made by Austria, Finland, Sweden and the United Kingdom, Explanatory Note, September 2002 Special Categories of Data Proposal (1)6, *available at* http://www.dca.gov.uk/ccpd/dpdamend.htm#part2

[106] *See id.* 同樣的困擾也存在資料主體的姓名上，某些特殊的姓氏即可辨識出其所屬種族。

[107] *See id.* 「歐盟個資指令」之規定也過度涵蓋「公開發行」的刊物，例如電話簿。

卻認為資料本身應是中性(neutral)的，資料處理的過程才有可能對基本自由與隱私造成侵害，此見解與釋字第 603 號解釋中余雪明大法官意見相似。

歐盟其他規範有參考「歐盟個資指令」訂有「敏感性個資」者，例如 2001 年發佈的「歐體機構與組織有關個人資料處理之保護與資料自由流動規章[108]」(Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data)其定義之敏感性個資與「歐盟個資指令」相同。2002 年發佈的「隱私與電子通信指令」(Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector)[109]則未對規定「敏感性資料」，僅於前言部分提到「使用者應有機會拒絕安裝cookies或類似裝置於他們的終端機系統(terminal equipment)。因為其他使用人將得以接觸該終端機系統與儲存於類似系統中之敏感性的資訊」。[110]此規定似認cookies有揭露敏感性個資之虞，第四章後詳。

五、APEC「隱私保護綱領」

2004年，亞洲太平洋經濟合作組織(Asia-Pacific Economic Cooperation, APEC)通過「APEC隱私保護綱領(APEC Privacy Framework)」。「APEC隱私保護綱領」

---

[108] 歐盟之立法方式可分為「規章」(Regulation)與「指令」(Directive)，前者具有一般適用性，直接拘束歐盟機構與各會員國；後者則保留較大空間，各會員國仍須透過制訂國內法以符合「指令」之要求，參見歐盟羅馬條約 The Treaty of Rome, 25 March 1957, Art.189.

[109] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[110] Directive 95/46/EC Ricital 25.

採取與「OECD個資綱領」相同之個資保護核心概念，[111]一般認為係繼「OECD個資綱領」後，建立了未來20年可資運用的個人資料保護原則。[112]「APEC隱私保護綱領」與「OECD個資綱領」相同，並未定義敏感性個資，[113]但在第三原則「蒐集限制」(Collection Limitation)後的評論(Commentary)曾提及敏感性個資，認為：**蒐集**「信用卡號碼」(credit card numbers)、「銀行帳戶資訊」(bank account information)或「**其他敏感性個人資訊**」(other sensitive personal information)**之方法**(collection methods)，**須**「**合法且公平**」(lawful and fair)，不得以「虛偽不實」(false pretenses)之方法蒐集資料。[114]本段評論似將「信用卡號碼」、「銀行帳戶資訊」等「財務資料」視為敏感性個資，為前揭各國際公約所未見。「財務資料」是否確屬「敏感性個資」，仍有疑義。

111 *See* Graham Greenleaf, *APEC's Privacy Framework: A new low standard*, 11(5) PRIVACY L. & POL'Y REP. 121-125 (2005).

112 *See generally* Graham Greenleaf, Five years of the APEC Privacy Framework: Failure or Promise?, 25 COMPUTER L. & SECURITY REV. 28 (2009).

113 兩公約多規定原則性的宣示，較少定義個資之相關概念，「OECD 個資綱領」僅定義「資料控制人」(data controller)、「個人資料」(personal data)與「個人資料之跨境流動」(transborder flows of personal data)；「APEC 隱私保護綱領」亦僅定義「個人資訊」(personal information)、「個人資訊控制人」(personal information controller)與「公開可利用資訊」(publicly available information)。

114 APEC Privacy Framework, Commentary 18.

第三節　各國立法例

截至 2012 年底為止，全球至少有 89 個國家訂有個人資料保護法或隱私法，[115] 以保護國內之個人資料，其中有關敏感性個資之規定，各國規定不一而足。歐盟各國由於受到「歐盟個資指令」之拘束，包括英國、德國等國皆訂有敏感性個資之規定，歐盟以外其他國家之立法，有仿效歐盟規定者，例如澳洲，亦有改採與歐盟不同觀點之美國、加拿大與日本。至於我國個資法，主要仿效德國、奧地利之規定，亦即同樣受到「歐盟個資指令」影響較大，以下以較受矚目之歐盟國家、美國、加拿大、澳洲、日本與我國，逐次探討其立法規範。

一、歐盟國家

原則上，歐盟各國之個人資料保護立法皆受「歐盟個資指令」拘束，各國所定義之敏感性個資大致與「歐盟個資指令」規範相符：僅限於顯示「種族血緣」、「政治意向」、「宗教或哲學信仰」、「工會會員資格」與涉及「個人醫療或性生活」等五類之個資。英國資料保護法(UK Data Protection Act 1998)第 2 條規定，敏感性個人資料係指與下列事項相關之個人資料：[116]

> 「資料主體之**種族或民族根源**；其**政治觀點**；**宗教信仰或其他相同性質之信仰**；是否為**工會之成員**；其**生理或精神健康或狀態**；其**性生活**；其

---

[115] *See* Graham Greenleaf, Global Data Privacy Laws: 89 Countries, and Accelerating, 115 PRIVACY L. & BUS. INT'L REP. 1 (2012).

[116] 例如英國資料保護法(§ 2)。事實上在「歐盟個資指令」通過以前，英國並未規範敏感性個資。1984 年，英國舊資料保護法雖曾授權國務院得發佈規則定義四種敏感性個資，惟該規則從未發佈。德國則透過衡平條款提供敏感性個資較一般個資更高的保護，參見 Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1351 n.198 (2000).

所犯罪行為或被指控之罪行；關於其犯罪行為或被指控罪行之訴訟結果或上訴判決。」

細觀各國規定，有關敏感性個資之定義存有兩點不同。第一，認定時點不同。亦即，個人資訊於「何時」得被視為敏感或特別資訊；第二，部分國家在「歐盟個資指令」的定義下，增加類別屬性相似的敏感性個資。

首先，關於用以規範個人與敏感性個資之關連文字，各國規定有所歧異。「歐盟個資指令」第 8 條規定，禁止處理「顯示」(reveals)種族血緣等之敏感性個資，歐盟多數國家採之；少數國家規定，禁止處理與種族血緣等「相關」(concerning)之資料。[117]使用不同文字來定義「本人與敏感性個資之關連」，將影響敏感性個資之認定，例如網路瀏覽紀錄可能不會「顯示」個人性生活偏好，但卻會與性生活偏好「相關」。較為特殊者，法國禁止處理「直接」或「間接」(indirectly)揭露種族血緣等之敏感性個資。[118]申言之，在某些情況下，直接購買猶太或伊斯蘭食品、購買雜誌或瀏覽網站之資訊，可能無法與「個人信念」或「性生活」產生相關，惟此行為卻可能「間接」顯示某些程度的敏感性個資。監視攝影機或影像紀錄器也有可能顯示某一個人的種族。[119]

其次，各國對於敏感性個資之定義，有兩點不同。第一，增加敏感性個資之

---

[117] 例如奧地利、德國採用「關於、有關」(on)；義大利特別強調「揭露的能力」(capable of revealing)；荷蘭採用「資料關於」(data concerning)；英國、愛爾蘭使用「關於」(as to)；希臘使用「相關」(relate to)；盧森堡規定較寬鬆，認為僅於「處理」敏感性個資時，始受到個資法之規範，參見 Korff, *supra* note 31, at 84-85.

[118] 法國資料保護法 §8(I)

[119] *See* Korff, *supra* note 31, at 84-85.

「方法」不同。通說認為，[120]「歐盟個資指令」規定係為「列舉」規定，各國應避免增加敏感性個資之類別，惟各國立法實踐上相當複雜，有另外於「得豁免禁止而予以處理」之情況下，另規範敏感性個資者，亦即在定義「敏感性個資」之條文外，另規定某類型資料禁止處理，除非符合豁免禁止之要件；[121]有直接在規範敏感性個資的同一條文內，直接增加其項目者。[122]第二，增加敏感性個資之「類別屬性」仍與「歐盟個資指令」相關。多數國家新增之「類別屬性」與個人醫療相關，例如「基因資訊」[123]、「治療資訊」[124]；將「刑事紀錄」列為敏感性個資；[125]將「工會會員資格」擴大適用；[126]新增「私人事務」(private matters)者。[127]

---

[120] *See* McCullagh, *supra* note 56, at 192, 197; RICHARD MORGAN & RUTH BOARDMAN, DATA PROTECTION STRATEGY: IMPLEMENTING DATA PROTECTION COMPLIANCE 2.2.2.1 (2003); Lee A. Bygrave, *Core Principles of Data Protection Laws*, *in* DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 344 (2002).

[121] 例如比利時：犯罪行為資料(§ 9)、瑞典：違法行為(§ 21(1))、丹麥：嚴重社會問題與純粹私人事務(§ 8(1))。此種（於豁免限制條款中新增類別）規範方法有產生矛盾衝突之疑慮，蓋各國規範敏感性個資之方式，是先定義概念，再設定豁免限制之條款，個資須先符合敏感性個資之定義，再適用豁免限制之條款予以處理或利用，如逕以豁免限制條款擴張敏感性個資，則有牴觸先前定義規定之虞。

[122] 例如英國「刑事判決」(§ 2(h))、葡萄牙「基因資訊」(§ 7(1))。此外，有兩者立法方法皆採用者，例如荷蘭於定義時新增「犯罪紀錄」(§ 16)，於豁免處理時另新增「遺傳特徵」(§ 21(7)).

[123] 例如盧森堡(§ 6(1))、荷蘭(§ 21(7))、冰島(§ 8(c))將「基因資訊」視為有關「健康」之資訊，盧森堡更進一步定義為「個人或群體個人之遺傳特質資訊」；葡萄牙則認為與「健康與性生活」相關(§ 7(1))。瑞典未將「基因資訊」視為敏感性個資，但其仍特別立法(Sweden, Act on Biobanks in Health Care (2002: 297))規定其處理方式，其餘參見 Korff, *supra* note 31, at 85.

[124] 芬蘭將有關「治療」(treatment)之資訊，視為敏感性個資，參見 Finnish, The Personal Data Act (523/1999) § 11(4).

[125] 例如比利時(§ 9)、瑞典(§ 21(1))、英國(§ 2(h))將刑事犯罪資料視為敏感性個資，參見 Korff, *supra* note 31, at 94. 比利時將處理之限制自「犯罪資料」(criminal data)擴大至「任何法律上爭議」(any legal disputes)。此類資訊得基於「法令明確規定之目的」(any purpose specified by law, decree or regulation)而予以處理。事實上，某些行為是否符合本款（刑事紀錄）規定，相當難以認定，例如警察逮捕現行犯之行為，參見 KUNER, *supra* note 34, at 2.96.

[126] 例如希臘「任何會員資格」(membership in any association)、義大利「政黨、商會協會會員資格」

值得注意的是，雖然各國有義務修正個資法以符合「歐盟個資指令」之要求，但事實上「歐盟個資指令」之規範與各國舊有之個資法規範並不相同。例如丹麥傳統上不將「工會會員資格」視為敏感性個資；[128]捷克未對「DNA樣本」有相關立法，但實踐上卻將其視為敏感性個資；[129]奧地利與德國原先對敏感性個資之認定係採取資料「情境」(context)判斷，而非「直接定義」。[130]

至於身份識別號碼，「歐盟個資指令」第8條第7項，雖規定會員國應決定**國民身份號碼**(national identification number)或其他**通用之識別號碼**(identifier of general application)之處理條件，[131]但本規定實際上並未影響「沒有國民識別號碼」之會員國個資法。關於本項規定是否適用於駕照號碼、國家保險號碼或護照號碼，仍有待商榷。因為上述這些號碼都不是「通用號碼」，它們都只是為了特定目的所存在。[132]個人識別號碼得用於「一般」或「特殊部門」，亦得由「公部門」或「私人」來使用。識別號碼的風險在於，僅使用一個號碼就可以獲得資料主體的不同資訊，[133]此特徵與「生物辨識資訊」幾乎相同。

(§ 22)。希臘更進一步將「社會福利」(social welfare)增訂為敏感性個資，參見 Greece, Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data Art.2(b)

[127] 丹麥(Art. 8.1)、葡萄牙規定有關「私人事務」(private matters)之資料為敏感性個資。葡萄牙憲法法院認為「錄影監視」(video surveillance)屬於接觸「私人事項」。該國主管機關亦認為「手機定位資訊」(phone positioning data)屬於敏感性個資，但純粹財務資訊則不屬之，參見 Korff, *supra* note 31, at 85.

[128] *See* Korff, *supra* note 31, at 84.

[129] *See* Lukáš Prudil & Josef Kuře, *Research Ethics Committees in the Czech Republic*, *in* RESEARCH ETHICS COMMITTEES, DATA PROTECTION AND MEDICAL RESEARCH IN EUROPEAN COUNTRIES 34 (2005).

[130] 此項爭議詳參本章第四節。

[131] Directive 95/46/EC, Art.8.7 "Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed."

[132] *See* DAVID BAINBRIDGE, EC DATA PROTECTION DIRECTIVE 58 (1996).

[133] *See* Ségolène Rouillé-Mirza & Jessica Wright, *Comparative Study on the Implementation and Effect*

二、其他國家

（一）美國

美國 1974 年制訂之「隱私法」(Privacy Act)[134]規範政府蒐集、處理及利用個人資料，其定義「紀錄…不限於教育背景、金融交易、**醫療病史**、**犯罪前科**、工作履歷與其他包含其姓名、識別號碼、代號或其他專屬於個人之識別資訊，例如**指紋**、聲紋與照片」，乃將前述「歐盟個資指令」之敏感性個資一併納入個人資訊之「紀錄」內，而未特別定義敏感性個資；[135]「公平信用報告法」(Fair Credit Reporting Act of 1970, FCRA) [136]規定：資料主體以「信用」(credit)、「僱傭」(employment)或「租賃審查」(tenant screening)之目的申請信用報告時，信用報告機構得蒐集敏感性較高之資料，例如醫療資訊；[137]「駕駛隱私保障法」(Drivers Privacy Protection Act, DPPA)規定：「照片」、「社會安全號碼」(Social Security Numbers, SSN)與「醫療資訊」不得任意使用；[138]「梅根法」(Megan's Law)規定：各州政府於一定情形時應公開性犯罪人士之資訊。[139]

---

of *Directive 95/46/EC on Data Protection in Europe: General Standards*, *in* THE DATA PROTECTION DIRECTIVE AND MEDICAL RESEARCH ACROSS EUROPE 158 (Deryck Beyleveld, David Townend, Ségolène Rouillé-Mirza & Jessica Wright eds., 2004).

[134] Pub. L. No. 93-579, 5 U.S.C. § 552a

[135] *See id*. § 552a(a)(4)

[136] Pub. L. No. 90-32, 15 U.S.C. §§ 1681 et seq. *See* FCRA, Sec. 603(w) & 612(a)(c)(i); ANITA L. ALLEN & RICHARD C. TURKINGTON, PRIVACY LAW: CASES AND MATERIALS 476(2000).

[137] Comparative Study of European Commission Directorate-General Justice, Freedom And Security on Different Approaches to New Privacy Challenges, In Particular in the Light of Technological Developments- B.1 – United States Of America, at 10 (May. 2010) *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf; 如該信用報告係分析自消費者之行為而非信用活動（例如貸款）者，則不受本法規範，詳情可參見 JON L. MILLS, PRIVACY: THE LOST RIGHT 142 (2008).

[138] Pub. L. No. 103-322, 18 U.S.C. §§ 2721-2725. *See* DPPA §§ 2722(a) & 2725(3).

[139] Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act of 1994.

美國對於敏感性個資之保護，缺乏統一立法規範。敏感性個資須依其類型，分別適用不同法規，故適用上常有疑義。以「醫療保險流通與責任法」(Health Insurance Portability and Accountability Act, HIPAA)[140]為例，該法雖專門規範醫療資訊之處理，但如由不受HIPPA規範之機構蒐集醫療資訊，即不受到任何保護，例如醫療產品機構處理顧客填寫之產品回函。因為該產品機構並非HIPPA所規範之主體，故可蒐集顧客之健康資訊，甚至出售該資料。[141]美國多數私人機構都可以購買、販售或辨識有關生理、心理狀況或政治意見等資料。[142]此外，目前並無任何專門規範社會安全號碼(SSN)使用之聯邦立法。[143]各州則有已立法進行規範其蒐集、處理及揭露者。[144]

由於歐盟禁止各會員國將資料傳輸至非達資料保護水平之國家，美國為保護其國內企業利益，能與歐盟間進行商業資料傳輸，由商務部(U.S. Department of Commerce)發佈「安全港協定」(U.S.-EU Safe Harbor Agreements) [145]，其中定義敏

相關討論參見 ALLEN & TURKINGTON, *supra* note 137, at 153-155.

[140] Pub. L. No. 104-191 (Privacy Rule promulgated at 45 CFR § 460).

[141] 其他類別之法律還有「有線通訊政策法」(Cable Communications Policy Act of 1984)規範有線電視業者蒐集「個人電視收看習慣」；「金融服務法」(Gramm-Leach Bliley Act of 1999)專規範金融服務機構所持有之個人資訊。

[142] 例如設立於喬治亞州的 ChoicePoint 公司，該公司專門將公共或私人資料庫中的個人資訊，公開販售給政府機關與私人企業，但這樣的情況在歐洲卻是違法的。目前該公司擁有多達 17 億筆個人資訊，10 萬名顧客，收益高達 1 億美元，參見 Maeve Z. Miller, Note, *Why Europe Is Safe from Choicepoint: Preventing Commercialized Identity Theft through Strong Data Protection and Privacy Laws*, 39 GEO. WASH. INT'L L. REV. 395-421 (2007). 該公司曾因揭露敏感性個資而遭聯邦貿易委員會(Federal Trade Commission, FTC)控告，詳情參見 MILLS, *supra* note 137, at 158-159.

[143] 根據隱私法第 7 條 Sec. 7(a) (1)，聯邦或州政府於揭露當事人社會安全號碼時，應予通知。

[144] 例如加州，詳細規定參見 California Office of Information Security and Privacy Protection, "Recommended Practices for Protecting the Confidentiality of Social Security Numbers," *available at* http://www.privacy.ca.gov/res/docs/pdf/ssnrecommendations.pdf

[145] 本協定係由美國商務部基於促進國際商業發展之法定職權所發佈，並於 2000 年 7 月經歐盟執委

感性個資為：與「醫療、健康資訊」、「種族血緣」、「政治意向」、「宗教或哲學信仰」、「工會會員資格」與「個人性生活」者，其定義與「歐盟個資指令」一致。「安全港協定」並規定機構組織應針對「敏感性資料」(sensitive information)提供當事人「同意加入(opt-in)」[146]之權利，以主動選擇是否願意將其敏感性個資提供給第三人。

美國聯邦參議員Patrick Leahy於 2011 年 6 月所提出「個人資料隱私與保障法」(The Personal Data Privacy and Security Act of 2011)草案[147]，將「可識別之敏感性個人化資料」(sensitive personally identifiable information)定義為：以電子化或數位形式所記載之下列資訊：1. 與「個人姓名」結合之「未經截斷(non-truncated)之社會安全號碼」(social security number)、「駕照號碼」(driver's license number)、「外國人登記號碼」(alien registration number)、住家地址、電話號碼、母親本姓(Mother's maiden name)、出生日期、「獨特之生物辨識資訊」(unique biometric data)，例如「指紋」(finger print)、「聲紋」(voice print)、「虹膜或視網膜圖像」(retina or iris image)、「其他獨特的物理特徵」(any other unique physical representation)、「獨特之帳戶識別碼」(unique account identifier)、電子識別號碼、使用者名稱或「以獲取金錢、商品、服務或任何有價值之物所必要，而結合安全代碼(security code)、近用代碼(access code)或帳戶密碼(password)之序列代碼(routing code)；2. 財務帳戶名稱與「以獲得信用(credit)、撤銷貸款(funds)或從事財務移轉所必要，而結合安全代碼(security

---

會同意批准(Commission Decision 2000/520/EC, 2000 O.J. (L 215)7) 遵守本協定之美國機構，皆可視為已達到「歐盟個資指令」之保護水平。有關本協定，參見 International Safe Harbor Privacy Principles, *available at* http://export.gov/safeharbor/eu/eg_main_018475.asp

[146] 詳情參見本文第四章。

[147] 草案原文 *available at* http://www.leahy.senate.gov/imo/media/doc/BillText-PersonalDataPrivacyAndSecurityAct.pdf

code)、近用代碼(access code)或帳戶密碼(password)之信用卡或轉帳卡號碼」。[148]草案所規範之敏感性個資，似皆為中性(neutral)之個資，不帶有主、客觀價值判斷，與「歐盟個資指令」規範迥異。

（二）加拿大

加拿大之個人資料保護法，依據適用對象不同分為「隱私法」(Privacy Act, PA)[149]與「個人資訊保護暨電子文件法」(Personal Information Protection and Electronic Documents Act 2000, PIPEDA, 下稱「個資法」)。前者適用於聯邦政府機關，後者適用於私人機構。加拿大「隱私法」將個人資料定義為，「有關可得識別之個人訊息，而以任何形式紀錄以下事項：

(a) 有關**種族、國家民族根源**或膚色、**宗教**、年齡或婚姻狀況之資訊；

(b) 有關教育或**醫療、刑事**與個人就業紀錄與個人涉及財務交易之資訊；

(c) 任何得識別之號碼、象徵或其他特徵；

(d) 個人地址、**指紋**或血型；

(e) 個人意見或觀點；…」

上開定義不僅包括一般常見之敏感性個資，尚及於其他一般個人資料。此外，加拿大「個資法」將「個人資料」廣泛定義為，「屬於可得辨識之個人資訊，並排

[148] § 3(12)(A)(3) (iv)("A unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, or password if the code or password is required for an individual to obtain money, goods, services, or any other thing of value; or…).

[149] R.S. 1985, c. P-2

除公司地址與受僱人電話號碼等」，[150]並未特別定義敏感性個資。就此理解，加拿大之立法與前揭美國立法有相同之處，兩者定義之「個人資料」（加拿大）或「紀錄」（美國）皆涵蓋通說之敏感性個資。

值得注意者，在「個資法」後所附之「模範個資準則」(Model Code for The Protection of Personal Information) [151]規定，私人機構於決定「當事人同意之形式」時，例如以書面或口頭同意，應考慮**資訊之敏感性**(sensitivity of information)。[152]亦即，賦予機關裁量權以決定該資料是否為敏感性個資。[153]該點說明並謂：「儘管有些資料一直被認為是敏感性個資，例如**醫療紀錄**(medical records)或**所得紀錄**(income records)，但任何資料**依據其情境**(context)，都有可能是敏感資料。新聞雜誌訂購者之姓名與地址通常不會被視為是敏感性個資，而某些特殊種類的雜誌可能就會被視為是敏感性個資，例如與宗教或種族相關」。[154]此概念與「歐盟個資指令」所採之規範原則不同。申言之，「歐盟個資指令」定義敏感性個資係直接列舉特定內容，而加拿大「個資法」賦予機構**依據其情境**自行認定資訊是否具備「敏感性」而為敏感性個資，如此將使敏感性個資之定義大幅擴張。蓋加拿大並未特

---

[150] Canada PIPEDA § 2(1)

[151] Canada PIPEDA Sch.1 PRINCIPLES SET OUT IN THE NATIONAL STANDARD OF CANADA ENTITLED MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION, CAN/CSA-Q830-96. (“In determining the form of consent to use, organizations shall take into account the *sensitivity* of the information”) (emphasis added).

[152] *See id.* Sch.1(Sec.5) 4.3.4

[153] *See* CANADIAN INSTITUTES OF HEALTH RESEARCH, QUESTIONS AND ANSWERS FOR HEALTH RESEARCHERS 14 (2001), *available at* http://publications.gc.ca/collections/Collection/MR21-25-2001E.pdf

[154] *See* PIPEDA Sch.1(Sec.5) 4.3.4 (“Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the *context*. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive”) (emphasis added).

別定義敏感性個人資訊，且「個資法」之「個人資訊」定義廣泛，已包含一般通念上所認之敏感性個資。交由私人機構認定之資訊，已不限於所謂敏感性個資，而係一般個人資訊。故經該機構認定之敏感性個資，將有可能是一般個人資訊，僅因其具備「敏感性」而已，此為加拿大立法特別之處。

（三）澳洲

澳洲於 1988 年制定「隱私法」(Privacy Act)。[155]該法受「OECD個資綱領」之影響，建立 11 種適用於多數聯邦政府之「資訊隱私原則」(Information Privacy Principles, IPPs)，[156]其中並未區別一般個人資料與敏感性個資。[157]1995 年，「歐盟個資指令」促使澳洲於 2001 年發佈規範私人機構之「國家隱私原則」(National Privacy Principles, NPPs)。[158]澳洲「隱私法」將敏感性個資列為數種，包括：[159]

1. 關於下列事項之個人之資訊或意見：**種族或人種根源；政治意見；政治性社團之會員資格；宗教信仰或聯繫；哲學信仰；專業性或商會會員資格；工會會員資格；性偏好與性行為；刑事紀錄**；或
2. **個人健康資訊；**或
3. 不屬於前項之**個人基因資訊**

「澳洲法改會」(Australian Law Reform Commission, ALRC)認為敏感性個資需特別保護之原因，在於該資訊高度個人化(highly personal)且可能構成不正當的歧視

---

155 Australia Privacy Act 1988

156 *See id.* Part II Division 2

157 *See* 3 AUSTRALIAN LAW REFORM COMMISSION, FOR YOUR INFORMATION: AUSTRALIAN PRIVACY LAW AND PRACTICE 62.2 (2008).

158 *See* Australia PA Sche.3 10

159 *See id.* § 6 (sensitive information)

(unjustified discrimination)，[160]並建議將其定義擴張至「生物辨識資訊」(biometric information)[161]，因為「生物辨識資訊」**具有其他敏感性個資之特質，且透過該資訊可獲得更多敏感性個資**。[162]澳洲「國家衛生暨醫療研究委員會」(National Health and Medical Research Council, NHMRC)建議，定義敏感性個資時，應保持適當彈性。[163]澳洲「科學與工業研究研究組織」(The Commonwealth Scientific and Industrial Research Organisation, CSIRO)建議敏感性個資應包括「文化性敏感性資料」(culturally sensitive data)或其他被資料提供者（本人或他人）視為敏感性之資訊。[164]

另，在「隱私法」第 18E 章有關信用報告(credit reporting)規定中，認為個人之信用資料**不得**包含：

(a) **政治、社會或宗教信仰與聯繫**；

(b) **刑事紀錄**；

(c) **醫療病史或身體障礙**(physical handicaps)；

(d) **種族人種或國家根源**；

(e) **性偏好與性行為**；

(f) 生活習慣、人格特質與名聲。

此項分類與前述敏感性個資相當類似，惟本項分類缺少「健康資訊」，且增加了「生活習慣」、「人格特質」與「名聲」等項目。[165]「澳洲法改會」認為這兩項

---

[160] *See* 1 ALRC, *supra* note 32, at 6.95.

[161] *See id*. Recommendation 6-4 其分別為：以自動化生物檢測或辨識系統為目的所蒐集之生物資訊；生物樣本資訊。

[162] *See id*. at 6.119.

[163] *See id*. at 6.99.

[164] *See id*.

[165] 參見澳洲隱私法 § 18E(2).

定義有目的性的差異，前述（NPPs第 10 點）之禁止蒐集係避免在**未獲個人同意**下進行蒐集，而本項（信用報告）係完全禁止蒐集，無論有無獲得當事人同意。[166]就此理解，「澳洲法改會」似認「生活習慣、人格特質與名聲」其保護利益高於「健康資訊」，應絕對禁止列於信用報告中。

（四）日本

日本之資料保護法並未定義敏感性個資。2003 年制定的「個人資料保護法」[167]，規定個人資料處理之基本原則，並適用於公務機關及私人機構。其第 2 條定義「個人資料」為與自然人有關之資訊，且該資訊得以姓名、出生日期與其他內容可得識別出自然人之身分者（包括得輕易與其他資料對照而識別出自然人之資訊）。同時，針對行政機關與獨立行政法人，亦另訂定「行政機關持有之個人資料保護法」[168]與「獨立行政機關持有之個人資料保護法」。[169]兩者之個人資料定義與「個人資料保護法」幾乎相同。敏感性個資之規定（定義與豁免），皆未見諸於上開三部法律中。

惟根據「個人資料保護法」第 6 條規定，政府應根據個人資料之**性質**與**利用方法**，採取必要之立法或保護措施。是以，2004 年經濟產業省與厚生勞動省共同發佈一份「經濟產業之個人資料保護方針」（経済産業分野ガイドライン），該方針認為當具有敏感性議題之個人資料洩漏時，各產業部門應立即通報經濟產業省，

---

166 *See* 3 ALRC, *supra* note 157, at 56.81.

167 個人情報の保護に関する法律，平成 15 年 5 月 30 日法律第 57 号。相關立法經過可參見林素鳳，〈日本個人資訊保護之法制化〉，《黃宗樂教授六秩祝賀—公法學篇（一）》，頁 107-135（2002 年 5 月）。

168 行政機関の保有する個人情報の保護に関する法律，平成 15 年 5 月 30 日法律第 58 号。

169 独立行政法人等の保有する個人情報の保護に関する法律，平成 15 年 5 月 30 日法律第 59 号。

包括：[170]

(a) 與其**思想、信念與宗教**相關者；

(b) 例如**種族、國籍、家庭根源**、戶籍地(registered domicile)、**生理與心理診斷、刑事紀錄**等會引起社會歧視者；

(c) 與團體行為相關者，例如**勞工行使組織、集會與協商之權力**；

(d) 與行使政治權力相關者，例如參與遊行，或行使請願等其他權力；

(e) 與健康照護或性生活相關者。

爾後，2007 年金融廳發佈「金融機構個人資料保護方針」[171]，其第 6 條「敏感性資料」規定「各金融部門不得蒐集、使用或提供給第三人下列資訊：

政治意見、**宗教（包括思想與信念）；工會活動之參與；種族、家庭根源、戶籍地；健康照護、性生活；刑事紀錄。**」

隨後並規定八種得豁免禁止得予處理之情形。綜上，日本所採取之規範方法類似美國、加拿大，但又有所差異。兩者皆無原則性之敏感性個資定義（皆屬於個人資料），且將不同特質之資料委由不同法規處置，惟美國、加拿大之保護層級仍停留在法律位階，日本則僅存於行政命令之層次，保護略顯不足。

---

[170] *See* Ministry of Economy, Trade and Industry, *Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information* 36 (2009), *available at* http://www.meti.go.jp/policy/it_policy/privacy/0910english.pdf

[171] *See* Financial Services Agency, *Guidelines for Personal Information Protection in the Financial Field* Art. 6, *available at* http://www.fsa.go.jp/frtc/kenkyu/event/20070424_02.pdf

（五）我國

我「舊個資法」未特別規定敏感性個資。「舊個資法」第 3 條規定：「個人資料：指自然人之姓名、出生年月日、身分證統一編號、特徵、**指紋**、婚姻、**家庭**、教育、職業、**健康**、**病歷**、財務情況、社會活動及其他足資識別該個人之資料」。2010 年新修正公布之「個資法」則增加「護照號碼、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式」七項例示規定。

「個資法」第 6 條規定「有關**醫療、基因、性生活、健康檢查、犯罪前科**」為「特種資料」。立法說明謂：

「按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、處理或利用，**恐會造成社會不安或對當事人造成難以彌補之傷害**。是以，一九九五年歐盟資料保護指令(95/46/EC)、德國聯邦個人資料保護法第十三條及奧地利聯邦個人資料保護法等外國立法例，均有特種（敏感）資料不得任意蒐集、處理或利用之規定。經**審酌我國國情與民眾之認知**，爰規定有關醫療、基因、性生活、健康檢查及犯罪前科等**五類**個人資料，**其蒐集、處理或利用應較一般個人資料更為嚴格**，須符合所列要件，始得為之，以加強保護個人之隱私權益。又所稱「性生活」包括**性取向**等相關事項，併予敘明」。

綜上，我「個資法」係基於「某些個人資料之性質較為特殊或敏感」，任意由資料控制人（公務機關或非公務機關）蒐集、處理或利用，將對資料主體（本人）造成傷害，故參酌「歐盟個資指令」與各國立法例，訂定敏感性個資。惟與前述「歐盟個資指令」與各國立法例比較，仍發現如下疑義：

1. 「醫療」或「健康檢查」資料應解為「與個人健康相關」之資料？

按「個資法施行細則草案」第 4 條第 2 項，定義「醫療之個人資料」，係「指**除前項病歷以外**，其他以治療、矯正或預防人體疾病、傷害、殘缺為目的，所為之診察、診斷及治療；或基於診察、診斷結果，以治療為目的，所為之處方、用藥、施術、或處置等行為全部或一部所產生之個人資料」。換言之，似指「**進行醫療行為所產生」之個人資料**。同條第 5 項定義「健康檢查之個人資料」為：「對於無明顯疾病症狀，非出於對特定疾病診斷或治療之目的，以**醫療行為**所為診察行為之全部或一部之總稱」，同樣亦屬「進行醫療行為所產生」之個人資料，兩者之定義不易區分，其差別僅在於：「健康檢查」之資料限於「對外觀健康之人，非以特定疾病之診斷為主要目的」者。[172]

各國立法例對於「健康資料」定義廣泛。所謂「健康資料」，英國資料保護法定義為：「個人主體之生理、心理健康或狀況」；[173]美國「健康保險責任法」認為醫療資訊係所有口頭或以任何形式記錄下的醫療資訊，包含：一、由醫療提供者、醫療保險公司、公共衛生主管機關、雇主、壽險業、學校或大學、醫療交易或資訊機構建立或接收之資訊。二、**與個人過去、現在、或未來身心健康相關資訊**；向個人提供的醫療保健資訊；或是支付過去、現在或未來個人醫療保健付款的資訊。[174]加拿大「個資法」雖未定義敏感性個資，卻特別定義「個人醫療資訊」，為關於個人無論其存亡之下列資訊：「**有關個人生理或心理之健康資訊**；有關個人所被提供之醫療服務資訊；有關個人捐贈其任何部分之身體、身體器官或基於測試、實驗而得之資訊；有關個人被提供醫療服務過程中所蒐集之資訊；向個人提供醫

[172] 參照「個資法施行細則草案」第 4 條之說明。

[173] 英國資料保護法 § 30(1)參見 COPPEL, *supra* note 34, at 5-059.

[174] HIPPA § 1171(4)

療服務者附帶蒐集之資訊」。[175]此外，歐洲法院(European Court of Justice) 於Lindqvist案，將健康資料擴大解釋，認為**包含與個人生理或心理健康狀態方面有關的訊息**。[176]

本文認為，為求徹底保護資料主體（本人），且避免兩者（「醫療」與「健康檢查」資料）適用之疑義（不易區分且無區分實益），「醫療」或「健康檢查」資料應採廣義解釋，共同理解為「與個人健康相關」之資料，並建議刪除「個資法」第 6 條第 1 項敏感性個資之「醫療」與「健康檢查」例示，改新增「健康」之例示。

2. 「病歷」為「敏感性個資」？

我「個資法」第 2 條將「病歷」視為個人資料之例示，而第 6 條定義之「敏感性個資」卻不包含「病歷」，將「病歷」排除敏感性個資之外，顯有疑義。我國法上之病歷包含兩種，第一種為「醫師依醫師法所製作」之病歷，包含下列事項：「一、就診日期。二、主訴。三、檢查項目及結果。四、診斷或病名。五、治療、處置或用藥等情形。六、其他應記載事項」；[177]另一種為「醫療機構建立」之病歷，包括：「一、**醫師依醫師法執行業務所製作之病歷**。二、**各項檢查、檢驗報告資料**。

---

[175] Canada PIPEDA § 2(1)

[176] ECJ Case C-101/01 本案被告為瑞典某教堂之兼職人員，其於網路上發佈含有教區教堂成員名單的網頁，包括成員姓名、工作、興趣與電話號碼等，其中包含某位人員因腳傷而請假的紀錄。瑞典法院認為被告非法處理敏感性個資。被告不服提起上訴，該上訴法院請求歐洲法院對於「歐盟個資指令」之適用作出解釋。該案爭點是：發佈腳傷者資料，是否構成處理敏感性個資中之健康資訊。

[177] 參照醫師法第 12 條。

三、**其他各類醫事人員執行業務所製作之紀錄**」，[178]其範圍較前者「醫師所作之病歷」更為擴大，且事項皆與「醫療資料」相關，更涵蓋「健康檢查」之資料，「個資法施行細則草案」第 4 條第 1 項，參照上開「醫療機構建立之病歷」為相同之規定。惟「個資法施行細則草案」之規定，仍值商榷。蓋「個資法施行細則草案」特地區分「病歷」與「醫療」資料兩者關係，將「病歷」排除敏感性個資定義之外；[179]且上開定義第二款所謂「檢查、檢驗報告資料」意義上屬於「健康檢查」之資料，如按「個資法施行細則草案」之解釋，將使「個資法」定義之「病歷」卻又涵蓋「健康檢查」之資料，使「病歷」與「健康檢查」資料之意義重疊。

綜上所述，「個資法」第 6 條第 1 項將「健康檢查」與「醫療」資料列為敏感性個資，卻未將「病歷」一併列入敏感性個資，本文認為係立法疏漏，[180]鑑於「醫療」用語之定義較「病歷」廣泛，「健康檢查」之資料亦屬「病歷」資料之一部分，三者概念上皆有所重複，[181]故建議將「病歷」視為「健康資料」（包含醫療與健康檢查資料）之部分，無須刻意將「病歷」排除敏感性個資定義之外。

3. 「基因」、「犯罪前科」與「性行為」之定義？

---

[178] 參見醫療法第 67 條第 2 項。

[179] 「個資法施行細則草案」第 4 條第 2 項，定義醫療之個人資料，係指**除前項病歷以外**，其他以治療、矯正或預防人體疾病、傷害、殘缺為目的，所為之診察、診斷及治療；或基於診察、診斷結果，以治療為目的，所為之處方、用藥、施術、或處置等行為全部或一部所產生之個人資料。

[180] 參見余啟民，〈由肺結核病患名單資料外洩談公務機關就醫資訊管控與監督〉，《月旦民商法雜誌》，24 期，頁 8-9（2009 月 6 月）；財團法人資訊工業策進會科技法律研究所，《給科技研發與創新服務提供者的—個資運用藍圖》，頁 88（2011 年初版）。

[181] 經查各國立法例並未存在將「病歷」排除醫療資料（敏感性個資）之實例。

「基因」資料所指為何，遍查我國法規並未出現相同用語，僅有「去氧核醣核酸採樣條例」提及「基因特徵」，並將其視為「儲存於去氧核醣核酸內之資料」。[182]「個資法施行細則草案」第 4 條第 3 項，定義「基因之個人資料」係指由一段去氧核醣核酸構成，為生物體控制特定功能之遺傳單位訊息。歐盟則將「基因」視為「任何形式之個人遺傳特徵」或「關連群體間之遺傳特徵」。[183]

「犯罪前科」之定義，參照「個資法施行細則草案」，所謂「犯罪前科」為指經**緩起訴、職權不起訴**或法院判決有罪確定之紀錄，[184]惟此定義仍有疑義，蓋緩起訴與職權不起訴皆非有罪判決之結果，能否一概視之為「犯罪前科」，尚須斟酌。「性行為」之定義，參照「個資法施行細則草案」，係指性取向或性慣行之個人資料。[185]

[182] 參照「去氧核醣核酸採樣條例」第 3 條第 3 款。

[183] Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data para 1, *available at* https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=564487&SecMode=1&DocId=560582&Usage=2

[184] 參照「個資法施行細則草案」第 4 條第 6 項。此定義係參考「行刑累進處遇條例個資法施行細則」第 8 條；另，「舊個資法」未將「犯罪前科」列為禁止處理之敏感性個資，故實務上曾有徵信業者進行蒐集、處理及利用之情形，參見法務部 93 年 7 月 26 日法律決字第 0930027495 號函。

[185] 參照「個資法施行細則草案」第 4 條第 4 項，草案修正說明謂：本定義係參考澳洲立法例，參見 1 ALRC, *supra* note 32, at 6.122.

第四節　敏感性個資之界定方法

綜觀前述國際規約與各國立法例，有關敏感性個資之界定方法，[186]略可分為以下兩種：

一、法律列舉模式

「列舉說」以個人資料之「內容」(content)定義敏感性個資。本說認為基於某些資料之「性質」(nature)，該資料之內容一旦揭露後，可能對個人隱私產生極大傷害，[187]包括引起恣意歧視。故針對某些內容之資料，立法禁止蒐集、處理或利用之。「歐盟個資公約」解釋報告(Explanatory Report)認為：「通常情況，資料處理會對人產生傷害，並不是基於該資料之內容，而係該資料之『使用』方式，但**某些特殊類型資料**，其『**本質**』很可能傷害到個人之權利與利益，本條（按：公約第 6 條）所列舉之特殊類型資料，在各會員國內通常被認為特別敏感」；[188]「歐盟個資指令」序言亦宣示「除非資料主體明確同意，否則依資料之性質將有可能

---

[186] *See* McCullagh, *supra* note 56, at 198-200.

[187] *See* Casabona, *supra* note 34, at 37; Lee A. Bygrave, *The Place of Privacy In Data Protection Law*, 24 U.N.S.W.L.J. 277, 280 (2001).

[188] Directorate General of Human Rights and Legal Affairs, Data Protection: Compilation of Council of Europe texts, para.43 *available at* http://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf (“While the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests. Categories of data which in all member States are considered to be especially sensitive are listed in this article”). 此見解似與釋字 603 號解釋林子儀大法官之「協同意見書」相似（蓋指紋具有許多適用於人別辨識與認證之特性，國家得藉由指紋以掌控國民行蹤）。

侵害基本自由與隱私者，禁止處理之」。[189]此說為目前立法主流，我國、歐盟國家（英、德）、澳洲立法例皆以此方法定義敏感性個資。

本說之優點在於，使資料控制人（公務機關或非公務機關）或資料主體（本人）得迅速自資料**內容**具體判斷，何者須禁止蒐集、處理或利用，或須遵循不同（更嚴格）之資料保護原則，有益個人資料保護之落實。其缺點在於資料之內容與形式會隨著社會、歷史與文化有所變動，[190]且無須考量資料主體（本人）之意見，[191]有可能過度保護，也有可能保護不足。

過度保護係指內容定義過廣，例如「歐盟個資指令」定義之「工會會員資格」，北歐國家傳統上並不將其視為敏感性個資，民眾對此也不關心。[192]同樣，「歐盟個資指令」所規範之「種族血緣」資料，於我國也可能不具太大的敏感性；反之，「歐盟個資指令」所規範之「政治意見」，雖未屬我「個資法」所定義之敏感性個資，但「政治意見」之個資於我國社會中具有之敏感性，其實並不亞於「健康檢查」

---

189 Recital 33 “Whereas data which are capable by their *nature* of infringing fundamental freedoms or privacy…” (emphasis added).

190 *See* European Commission's Information Society and Media Directorate-General, EU study on the Legal analysis of a Single Market for an Information Society, Chap.4 –Privacy and Data Protection 4.7 (Nov. 2009), *available at* http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=842 有學者認為「敏感性」係兼具主觀與客觀內涵之一種價值。價值為人類從事事務或與個人行為、習俗制度、商品貨物或服務相關之特質。敏感性的主觀內涵取決於「作成決定之個人」；客觀內涵則獨立於「作成決定之個人經驗以外」，此時價值都只是部分的，屬於行為的一部份或考慮中的目的，這兩種衝突的觀點往往會透過公共政策制定程序予以調和。參見 McCullagh, *supra* note 56, at 197.

191 *See* Carlisle Adams, *A Classification for Privacy Techniques*, 3(1) U. OTTAWA L. & TECH. J. 35, 40 (2006).

192 *See* Simitis, *supra* note 56, at 6.

等個人健康資料。澳洲的著名律師事務所DLA Phillips Fox認為，引進更多有關敏感性個資的概念，會導致該概念的濫用且削弱各機構據實踐隱私法之能力。[193]此外，某些資料係以照片、聲音、姓名或電話簿方式呈現時，皆有可能顯示資料主體之種族、國籍或健康狀況，如此仍將該照片、聲音或姓名視為敏感性個資，則有過度保護之嫌。「歐盟個資指令修正案」建議應參酌「歐盟個資指令」序言第 33 點，認為資料本身難以避免附帶顯示(incidental revelations of the characteristics)諸如「種族血緣」或「宗教或哲學信仰」等敏感性個資之特徵者，該資料不屬敏感性個資，以避免過度擴張敏感性個資。[194]至於，保護不足則指該清單所規範者過窄，不符需求。例如歐盟其他國家有自行新增敏感性個資，將「財務資訊」或「私人事務」列入者。[195]

根據英國資料保護署(The Information Commissioner's Office, ICO)進行的電話訪談，將已列入保護之「敏感性個資」與「非敏感個資」進行資料之「敏感性」調查，如表一所示。[196]

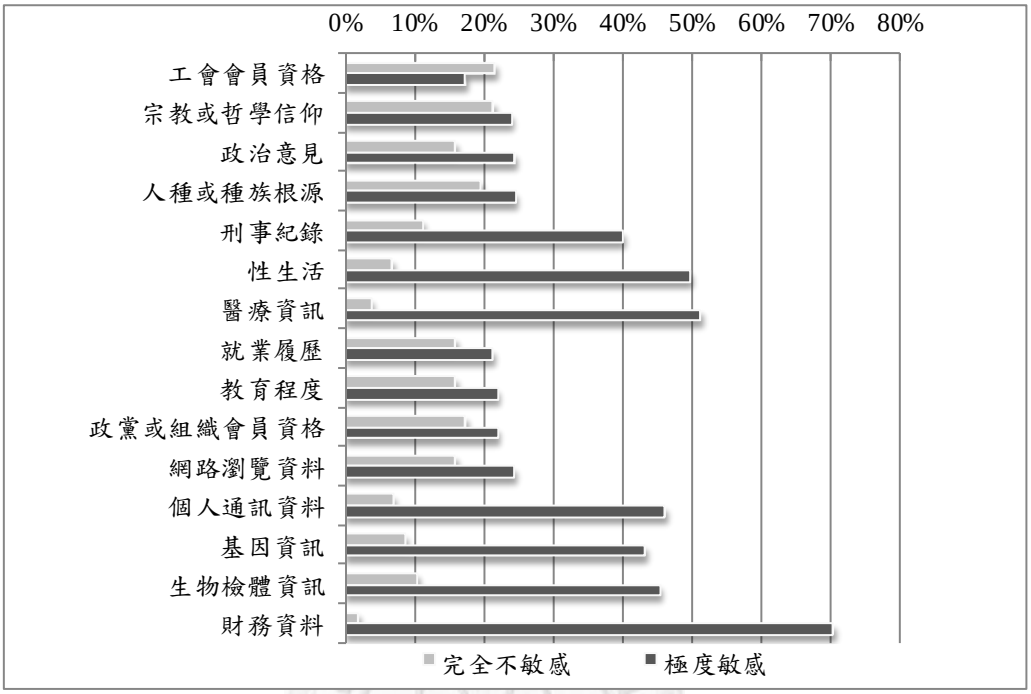
[193] *See* 1 ALRC, *supra* note 32, at 6.101

[194] Data Protection Directive (95/46/EC) Proposals for Amendment made by Austria, Finland, Sweden and the United Kingdom, Explanatory Note, September 2002 Special Categories of Data Proposal (1)6

[195] 例如芬蘭、葡萄牙、希臘，參見 Korff, *supra* note 31, at 85.

[196] *See* McCullagh, *supra* note 56, at 194-196.

表一：英國資料保護署敏感性個資訪談清單



資料來源：Karen McCullagh, *Data Sensitivity: Proposals for Resolving the Conundrum*, 2 J. INT'L COM. L. & TECH. 195 (2007).

上表係受訪民眾對於表內各類型之資訊，是否屬於敏感性個資之意見調查分析，本文僅擷取認為「完全不敏感」與「極度敏感」之數值表列。由上可知，多數人認為「刑事紀錄」、「性生活」、「醫療資訊」、「個人通訊資料」、「基因資料」、「生物辨識資訊」(Biometric Information)與「財務資料」為「極度敏感」之資料，尤其非屬「敏感性個資」之「財務資料」為本表最高。因此可簡單得出幾點結論：目前英國資料保護法所規定之敏感性個資清單有必要增修，且增加之類別係基於社會與科技發展而產生之資料。例如英國政府曾於 2001 年打算使用「生物辨識資訊」建立身份證，此一技術於先前發行身份證時尚未存在。[197]同樣的調查在我國

[197] 英國於二次大戰時曾發行過身份證，後於 1952 年終止。參見 *See* McCullagh, *supra* note 56, at 197.

有實施之必要，否則立法定義之敏感性個資將只是立法者想像中的敏感性個資，與民意可能產生脫節。此外，上述類別之資料，在我國並非廣泛的被視為敏感性個資，扣除「個資法」所規定之**醫療、基因、性生活、健康檢查、犯罪前科**外，本文認為，可考慮增加「政黨或組織會員資格」、「政治意見」以防此類資料每逢選舉即遭有心人士炒作，或增加「財務資料」以茲加強保護，避免詐騙橫生。[198]

最後，對於以上之困境，各國可採兩種方式加強保護，一則為修改法律，直接修正個人資料保護法或隱私法，增加敏感性個資之類別，並就特殊事項（例如醫療資訊）制定特別法，二則透過修法，授權行政機關發佈解釋函令。事實上，發佈解釋函令的方法最為有效、彈性，廣受各國採用。[199]例如荷蘭透過解釋函令，將有關「種族根源」之資料，擴大適用於「國籍」。[200]

二、綜合考量模式

（一）情境說(Context-based approach)

此說著重敏感性個資之「情境」(context)，主要立法例為依據「歐盟個資指令」修正前之奧地利與德國個資法。該說早於「OECD 個資綱領」時便與前「法律明文列舉說」成為兩大爭辯主流，最後使「OECD 個資綱領」放棄定義敏感性個資。

「情境說」認為敏感性個資並不是先驗(a priori)的概念。[201]**資料之敏感性並非與生俱來，任何資料根據其處理之情境，皆可具有一定之敏感性**，[202]故應針對「所

---

[198] 有認為應比照「歐盟個資指令」規範者，參見劉靜怡，〈不算進步的立法：「個人資料保護法」初步評析〉，《月旦法學雜誌》，183 期，頁 153（2010 年 8 月）。

[199] *See* Simitis, *supra* note 56, at 4.

[200] *See id*.

[201] OECD Guidelines' Explanatory Memorandum, para. 43 & 51; Bygrave, *supra* note 120, at 69 n. 263.

[202] *See id*. at 6; European Commission's Information Society and Media Directorate-General, *supra* note

有資料之處理情境」較敏感者，限制其使用。城仲模大法官於釋字 603 號解釋之「協同意見書」也表達類似的見解：「指紋本為中性之資料，單純知悉個人之指紋並無法透露任何訊息，蒐集指紋對於隱私權的影響如何，端視**指紋在個案中的用途而定**」。因此，考量資料之敏感性，應注意：**資料控制人之利益，資料接收者蒐集和處理之目的，資料處理之情形，**以及**資料處理對資料主體與控制人之影響**[203]，例如基因資訊或刑事犯罪資料對資料主體（本人）造成之損害。衡量「聲音」或「影像」資料之敏感性時，應合併考量其所載之「內容」，倘該資訊與個人性生活相關者，即具備敏感性。其他資訊，例如指紋或個人身份編碼，也應考量上開相關因素。

主張本說之學者認為，使用「列舉」之方法來規範敏感性個資，將徒勞無功。因為敏感性個資之定義會屢受挑戰，且從歐盟各國立法例觀察，僅有少數國家「完全」遵照「歐盟個資指令」之規定立法，多數國家仍新增屬於自己的敏感性個資。[204]學者建議，各國立法時應限制資料控制人使用敏感性個資，並明訂其蒐集之目的，且該蒐集限於必要之資料。[205]

英國資料保護官署(The Information Commissioner's Office, ICO)認為，個人資料之所以敏感，是因為資料處理的「環境」(circumstances)，而不是資料的「內容」(content)。傳統個資法將資料分為敏感性個資與一般個資，並將相關的良性資料

209, at Chap.2 4.32

[203] 對資料主體（本人）之影響除造成傷害外，尚有可能影響其決定，例如該資訊之不當散佈或揭露，而影響其原先被社群或家庭所期待之價值觀產生變化，參見 *See* Rein Turn, *Classif ication of Personal Information for Privacy*, NATIONAL COMPUTER CONFERENCE AND EXPOSITION 303-304 (1976).

[204] *See* Simitis, *supra* note 56, at 3.

[205] *See id*. at 8.

(benign information)以特別方法規範，顯有誤解。[206]澳洲「國家衛生暨醫療研究委員會」(National Health and Medical Research Council, NHMRC)認為，由於資訊之「性質」(nature of information)、處理該資訊之「情境」(context)及資料主體之意見，將使定義敏感性個資變得相當困難。資訊的敏感性(sensitivity)會隨著文化與個人而改變。[207]澳洲昆士蘭地方政府之「幼兒與青年保障委員會」(Queensland Government Commission for Children and Young People and Child Guardian)舉孩童受虐為例，認為一般醫師在接受到孩童因受虐或過失而受傷資訊時，會逕依醫療隱私之規範處理，將其視為醫療資訊，惟該資訊如由兒福工作者所接收，則該資訊即非單純之醫療資訊。所以，將孩童受虐資訊分類，除須考量資料之特質外，尚須考量其資料處理之「情境」(context)。[208]

值得注意者，「澳洲法改會」(Australian Law Reform Commission, ALRC)雖同意：資訊之敏感性會隨著其情境而變化，其卻反對修正澳洲隱私法原先之敏感性個資定義。因為**將敏感性個資一一列舉之規範方式實屬必然，且隱私法已就處理敏感性個資訂定更嚴格的要求**。[209]尤其現今隱私法與建議修正之「統一隱私原則」(Unified Privacy Principles, UPPs)內所規範的敏感性個資，一般情形須獲得本人同意始得蒐集，且僅得於原始蒐集目的內進行利用，進行其他目的利用時（二次目的），須與原始蒐集目的直接相關。此點亦與其他個人資料處理之規範不同（無須取得同意或可作目的外使用），所以（**列舉**）**定義敏感性個資始能清楚說明，該規範之適用對象**。[210]

---

[206] *See* Korff, *supra* note 31, at 85.

[207] *See* 1 ALRC, *supra* note 32, at 6.97.

[208] *See id*. at 6.100.

[209] *See id*. at 6.102.

[210] *See id.* at 6.103.

（二）目的說(Purpose-based approach)

理解此說必須先將「資料揭露」之概念自「資料處理」中獨立出來。本說主張，資料之「處理目的」為「揭露」具有「敏感性特質」之資訊時，該資訊即為敏感性個資，須受相關規定限制，敏感性是相對的。[211]本說著重的是**資料實際「處理目的」，而不是資料本身（內容）**。[212]本說認為，相同資料於不同情況下產生不同之敏感性，係個人使用之「意向」使然，而不是資料自身之本質產生變化。個人處理該資料時可能會考慮很多因素，例如誰能夠接觸此資料，且根據何種理由，而這樣的因素會導致該資料具備敏感性。例如警察可透過DNA資料以推論個人所屬之種族，但此工作卻不適合由私人機構執行，[213]此說與「OECD個資綱領」所提出「反對列舉敏感性個資」之主張類似。在「OECD個資綱領」B部分細節評論(detailed comments)的第七段「合法蒐集原則」曾謂：「…所有的資料，本質上都不具私人性或敏感性，僅在該資料處於**特定**的環境或**使用**時，始具備『私人』或『敏感性』」。[214]

本說最終目的在於，**防止他人恣意或非法的「揭露」「具有敏感特質」之資料，進而造成本人的傷害**，[215]例如購物網站蒐集消費者購買各類宗教書籍之偏好，其「處理目的」若為「揭露消費者之宗教信仰偏好」，則該資訊係屬敏感性個資；其「處理目的」若為「統計各類購書比例」，則該資訊將不屬敏感性個資。再例如，「處理目的」為藝術創作之街頭攝影，其攝影蒐集而得之行人照片，不屬敏感性

---

[211] *See* Jean-Marc Dinant et al., *supra* note 75, at 31.

[212] *See* McCullagh, *supra* note 56, at 199.

[213] *See id*.

[214] 參見前揭註 59 ("…it may be held that no data are intrinsically "private" or "sensitive" but may become so in view of their context and use.")

[215] 如試將「敏感性高」與處理「造成傷害高」相連結，則與釋字 603 號解釋許玉秀大法官「協同意見書」之見解類似（所謂資訊的敏感度，就是該資訊如果脫離個人控制[由他人進行處理]，可能對個人造成的損害有多大）。*See* Wong, *supra* note 57, at 12.

個資。此外，本說可減輕資料控制人於「資料保護機關」時的舉證責任，與減少瑣事案件進入法院的數量(*de minimis non curat lex*)。[216]亦即，資料控制人（公務機關或非公務機關）無須舉證證明該資料確以符合「例外得進行處理」之要件，僅須證明其「處理目的」並非意欲「揭露」「具有敏感特質」之資料即可。

本說之缺點為，在未定義「敏感性個資」之前，如何判斷該資料是否具有「敏感特質」，[217]而且如未能就敏感性個資先行定義，那所有資料都必須適用本目的論進行判斷，徒增困擾。本文以為，本說實際上是在定義後又增加一個豁免限制條款，亦即**敏感性個資之「處理目的」為「揭露」該資料，且「揭露」該資料不會對本人造成損害者，得例外予以處理**。

（三）合理說(Reasonableness-based approach)

本說認為，敏感性個資之定義已陳舊過時，故應綜合考量多種方法，以決定竟何者為敏感性個資。[218]例如立法者應考量處理個人資料之合理性。加拿大專門規範私人機構之「個人資訊保護暨電子文件法」(Personal Information Protection and Electronic Documents Act 2000, PIPEDA)未區分敏感性個資，其謂：「…制定蒐集、使用及揭露個人資料之規則，在某些程度上即承認個人對與其相關之個人資料擁有隱私權，且私人機構於蒐集、使用或揭露個人資料時之目的，須被合理之人認為適當」。[219]合理是一個客觀的標準，該機構必須考量資料處理之情況

---

[216] *See id*.

[217] *See* McCullagh, *supra* note 62, at 199.

[218] *See id.* at 200.

[219] Canada PIPEDA § 3 ("…rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances").

(circumstances)，且決定何者是「合理的」(reasonable)。資料處理之情況，可能包含**資料處理之背景**(context)與**處理資料之目的**(purposes)。是以，**本說不只採取合理性判斷，同時認為應兼採前述「背景說」與「目的說」**，例如在合理的情況下，貨運公司得要求不定期對其雇員（司機）進行酒精測試，以確保行車安全，但如該公司要求其雇員（司機）揭露任何與酒精相關之紀錄，則該資訊之揭露即屬不合理，因為其過於廣泛而且可能對受雇人產生傷害與歧視。本文認為，此說為「利益衡平」方法，包含以資料處理之「背景」、「目的」進行衡量，應保留予「具有決定權之資料主管機關或法院」，資料控制人如適用本說，將耗費過多人力資源判斷是否合法，無益於資訊之流動。

三、本文見解

（一）應考量資料之「性質」，以「法律明文列舉」方法界定敏感性個資

綜觀上開各國敏感性個資之規範方法，可知目前通說為：**法律明文列舉敏感性個資顯示之內容，例如醫療、基因或政治意見等個人資料**。列舉說主要考量：資料之「**性質**」(nature)，認為某些性質之資料，其內容一旦揭露後，可能對個人隱私產生極大傷害，故立法將其定義為敏感性個資。

採用「法律明文列舉」之好處在於，任何人皆得迅速自行判斷該資料是否屬於敏感性個資，有助於個人資料保護之落實。其他採用「情境說」(Context-based approach)或「目的說」(Purpose-based approach)等綜合判斷模式，事涉主觀，通常須交由公正之第三人（資料主管機關或法院）才能判斷。況且，我國缺乏統一的個人資料主管機關，如**將判斷敏感性個資之工作交由各類型的主管機關，敏感性個資之定義勢必形成歧異，無助於個人資料之保護，**

本文認為，**有關敏感性個資之定義方式，仍應以「法律明文列舉」之方式為**

宜，立法者應考量資料之「性質」，將顯示某些內容之資料列為敏感性個資。上開「綜合判斷模式」僅可供法院或將來有望成立之資料主管機關參考，於部分難以避免揭露敏感性特質，且通念上不屬於敏感性個資之資料，例如照片或姓名等，予以豁免適用之。

（二）指紋」應為「敏感性個資」？

近年隨著科技發展與社會文化變遷，藉由某些資訊形式已可辨識出更多的個人資訊，例如透過「生物辨識資訊」(Biometric Information)或「通用識別號碼」(identifier of general application)，將可獲得本人之醫療、種族等敏感性個資。[220]所謂「生物辨識資訊」，根據「澳洲法改會」之定義，係指包括「指紋」(fingerprints)，去氧核醣核酸(DNA)、虹膜(iris)、臉部特徵(facial features)、掌型(hand geometry)與聲音等資料。[221]一般而言，「生物辨識資訊」是固定不變的，[222]完全個人化且具有與其他敏感性個資共通的特質。[223]生物辨識資訊如遭誤用，可能導致非法之歧視，而且在未經本人同意下，進一步侵害本人之資訊隱私，[224]如此是否得將「指紋」或「生物辨識資訊」視為敏感性個資，本文認為仍有討論空間。

贊成將「生物辨識資訊」列為敏感性個資者，通常主張基於「生物辨識資訊」之「性質」，該資料之內容(content)一旦揭露後，可能對個人隱私產生傷害，而且

---

[220] 詳細討論可參見 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* 6 (2005), *available at* http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf

[221] 照片於某些程度上來說也是低程度的生物檢體資訊 *See* 1 ALRC, *supra* note 32, at 6.110.

[222] *See id*. 6.114

[223] *See id*. 6.119.

[224] *See id*. 蒐集「生物辨識資訊」之目的，應限使用於「自動化生物辨識」、「識別系統」與「生物模型資訊」(biometric template information)，*See id*. 6.1200

藉由掌握「生物辨識資訊」，將可辨識出更多的個人資訊。[225]反對者，則主張「生物辨識資訊」為一中性資訊，並不具有任何敏感性，僅有在特定情境下，該資料才會具有敏感性，[226]況且「生物辨識資訊」與「政治意見」、「宗教哲學信仰」等資料有別。蓋「政治意見」、「宗教哲學信仰」等資料通常可以一望即知該資料之內容，而「生物辨識資訊」則需要科學儀器的判讀，一般人掌握「生物辨識資訊」並無法立即顯示出資料之「敏感性」，仍須透過有心人士的操作或處理，始能充分掌握該資料之內容。

對此，本文認為「生物辨識資訊」縱然需特別處理，才能獲得資訊之內容，仍不影響該資料的性質(敏感度)。首先，在本章先前曾討論有關個人資料之定義，目前通說認為：個人資料係指資料控制人可識別出特定個人之資料，至於資料控制人有無能力識別該資料，則非所問，故即使資料控制人（一般人）取得「生物辨識資訊」後無能力識別特定人，而須交由其他具有辨識技術之資料控制人才能識別特定人，該「生物辨識資訊」仍屬個人資料，該**資料是否屬於敏感性個資與資料控制人有無能力辨識出特定個人，並無明顯的關連**。因為如果認為資料控制人須有能力自該資訊中識別出特定個人，該資訊才能作為敏感性個資，那一般人應該都無法自「醫療」或「健康檢查」資料中的血液檢測數值與「基因」資料中的基因排序資訊，獲得特定個人之資料，而使「醫療」、「健康檢查」與「基因」資料不屬敏感性個資，顯然與我「個資法」和各國實證立法規範相悖。

此外，查前揭各國立法，並無將「生物辨識資訊」列為敏感性個資之實例，

---

[225] 例如釋字 603 號解釋，林子儀大法官協同意見書認為指紋應為敏感性個資。

[226] 例如釋字 603 號解釋，余雪明大法官部分協同部分不同意見書，認為指紋為個人資訊之一種，指紋與隱私權無關，指紋僅為「中性之身分辨識工具」。

僅有美國與澳洲之修正草案，建議將「生物辨識資訊」列為敏感性個資。[227]此外，歐盟針對「歐盟個資公約」之研究報告，同時建議新增「識別號碼」(identification number)與「生物辨識資訊」(biological and biometric data)為敏感性個資。[228]可知將「生物辨識資訊」（包括「指紋」）列為敏感性個資仍屬於初步草案之提議，尚無統一之定論。

我「個資法」目前僅將「基因」（去氧核醣核酸(DNA)）列為敏感性個資，至於其他「生物辨識資訊」（例如「指紋」）則是屬於一般個資，非屬敏感性個資。本文認為，**「生物辨識資訊」之性質雖然與其他敏感性個資相似，但將「生物辨識資訊」視為敏感性個資之概念尚稱新穎，且此概念目前在國際間尚無明顯共識，故在立法者未獲得全民共識之前，本文暫不建議新增「指紋」或「生物辨識資訊」為敏感性個資。**

[227] 參見前揭註 160。

[228] 參見前揭註 75。

第五節　小結

本章所討論者為敏感性個資之概念。首先釐清，個人資料保護法中之相關概念；其次從國際規範與各國立法例，逐一檢視敏感性個資之概念。

相關概念中，個人資料係以「得以直接或間接方式識別自然人之資料」為準（個資法第 2 條第 1 款參照），不包含或「死者」之資料；有關「個資」之「操作」，概以「蒐集、處理或利用」稱之（個資法第 2 條第 3 款參照），並於本文第四章逐一檢視「敏感性個資」適用之「個人資料保護原則」。

「敏感性個資」之濫觴，為 1980 年 OECD 通過的「個人隱私與跨境個人資料流通保護綱領」與 1981 年歐洲理事會「保護個人關於自動化處理個人資料公約」。前者曾就敏感性個資之議題討論，後以該概念「不易釐清」而未予定義。後者則便首度定義敏感性個資並原則上禁止處理，惟該公約並未詳細規範（得豁免禁止而予以處理）之「例外情形」，且該公約對簽約國之強制力過低，使得各國資料保護水平未如預期。為了解決此一現象，並促進歐洲區域內的資料流動，歐盟於 1995 年通過「個人資料保護指令」，要求歐盟各國建立相同的個人資料保護水平。歐盟「個人資料保護指令」定義：敏感性個資為顯示種族血緣、政治意向、宗教或哲學信仰、工會會員資格之個人資料及涉及個人醫療或性生活等資料，並禁止會員國處理。此一概念影響歐洲各國之個人資料保護法，引導各國立法朝此方向修正，但因各國國情不同，仍有存在些許差異。

除前揭歐盟各國外，美國、加拿大與日本並未統一定義敏感性個資。美國係依照資料之性質交由不同法規規範；加拿大仍將其視為一般個人資料，僅賦予私人機構得根據資料之性質，自行認定資料之敏感性；日本則委由行政機關發佈規

則，規範不同類型之敏感性個資。澳洲法之定義與歐盟相同，「澳洲法改會」之修法告建議增加「生物辨識資訊」為敏感性個資。我「舊個資法」未定義敏感性個資，修正後之「個資法」則受歐盟「個人資料保護指令」影響，定義「有關醫療、基因、性生活、健康檢查、犯罪前科」之資料為敏感性個資。

綜觀如上各國立法例，可知目前各國規範敏感性個資之界定方法，略可分為兩種：「法律明文列舉」與「綜合考量模式」，後者又可細分為「情境說」、「目的說」與「合理說」。「法律明文列舉」係以資料之「內容」(content)來定義敏感性個資，認為基於資料之「性質」(nature)，該資料內容一旦揭露後，可能對個人之隱私產生極大的傷害，故直接列舉其內容項目並禁止蒐集、處理或利用。由於該列舉項目無法一應俱全，常遭受批評。有認為應考量資料處理之「情境(context)」，即資料控制人之利益，資料接收者蒐集和處理之目的，資料處理之情形，以及資料處理對資料主體與控制人之影響。有認為應僅考量資料處理之「目的」與合理綜合判斷上述情況者。

對於上開規範方法，本文認為：1. 維持我「個資法」規範現狀，考量資料之「性質」，以「法律明文列舉」定義敏感性個資，並適度參酌資料處理之「情境」，排除部分資料之適用（例如照片）；2. 修正「個資法」所定義之敏感性個資，建議新增「政黨或組織會員資格」、「政治意見」或「財務資料」以符合民情；3. 刪除「醫療」與「健康檢查」之用語，合併增訂為「健康」資料（包含「病歷」）。

第三章　敏感性個資之蒐集、處理及利用
—原則禁止、例外許可

第一節　禁止「蒐集、處理或利用」之原則

個人資料保護法之立法目的，在於確保個人之資訊隱私權、保護資訊安全流通，並提升資料處理之「究責可能性」(accountability)與「透明性」(transparency)。[229]對一般個人資料而言，個人資料保護法係為一「透明化之工具」(transparency tool)，使資料處理之過程向本人透明化，但對於敏感性個資而言，個人資料保護法則為一「非透明化之工具」(opacity tool)，[230]以立法限制或禁止國家、私人機構接觸敏感性個資。

蓋敏感性個資之公開或揭露將對個人「資訊隱私」造成較大之侵害，故針對敏感性個資，各國立法規範上採取與一般個人資料不同之規範方法，即**原則禁止資料控制人蒐集、處理或利用之，例外始得蒐集、處理及利用之**。我「個資法」第 6 條第 1 項亦同：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，**不得蒐集、處理及利用**」。

「歐盟個資公約」與「歐盟個資指令」皆「禁止處理(processing)」[231]敏感性

---

[229] *See* Nadezhda Purtova, *Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence, in* COMPUTERS, PRIVACY AND DATA PROTECTION: AN ELEMENT OF CHOICE 3.2.2 (Serge Gutwirth et al. eds., 2011).

[230] *See* Christel Beckman, *Regulating Privacy: Vocabularies of Motive in Legislating Right of Access to Criminal Records in Sweden, in* COMPUTERS, PRIVACY AND DATA PROTECTION: AN ELEMENT OF CHOICE 115 (Serge Gutwirth et al. eds., 2011).

[231] 此處所謂「處理」(process)應為廣義之處理，包含「蒐集」與「利用」之概念，參照「歐盟個資指令」第 2 條規定：「個人資料處理」指對個人資料所進行之任何或一系列操作，無論其是否以自動化方法進行，例如**蒐集**、記錄、組織、儲存、改編或修改、回復、參閱、**使用**、以傳

個資。「歐盟個資公約」第 6 條規定：「除各會員國國內法已提供適當安全措施者外，[各締約國]**禁止**對**顯示**下列內容之個人資訊，進行自動化處理…」。[232]「歐盟個資指令」第 8 條亦規定：「各會員國應**禁止**處理：**顯示**種族血緣、政治意向、宗教或哲學信仰、工會會員資格之個人資料及涉及個人醫療或性生活之個人資料」[233]。惟對於刑事紀錄之處理，「歐盟個資指令」並未直接禁止，僅規定：關於犯罪、刑事判決或保安處分等資料之處理，**限由公務機關監管下進行之**，或**國家法律已提供適當特定之安全維護措施者，會員國得訂定權宜條款**(derogations)。但刑案有罪判決之完整紀錄，應**由公務機關監管**。[234]2012 年「歐盟執委會」(European Commission)提出「個人刑事資料保護指令」草案，以規範各國主管機關(competent

---

輸或**散佈**而**揭露**或以其他使其有效的結合或排列、封鎖、消除與破壞，可茲參考。("processing of personal data" ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction).

[232] Convention 108 Art.6 "Personal data revealing *racial origin, political opinions or religious or other beliefs*, as well as personal data concerning *health or sexual life*, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to *criminal convictions*." (emphasis added).

[233] Directive 95/46/EC Art.8.1 "Member States *shall prohibit the processing* of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." (emphasis added).
本條之規定與某些會員國之憲法規定產生連結。例如西班牙憲法規定，認為「無人得以被要求揭露其宗教或信仰」與「禁止單獨創造記載『意識型態、工會會員資格、宗教信仰、種族血緣或性生活』相關資料」，丹麥亦有類似的規定。葡萄牙憲法特別就敏感性個資之儲存予以限制，參見 Korff, *supra* note 31, at 7.2

[234] Directive 95/46/EC Art.8.5 "Processing of data relating to *offences, criminal convictions* or *security measures* may be carried out only under the control of official authority, or if *suitable specific safeguards* are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority." (emphasis added).

authorities)處理有關「刑事犯罪之預防、調查、偵察與起訴」(prevention, investigation, detection or prosecution of criminal offences)與「刑罰之執行」(the execution of criminal penalties)之個人資料。[235]

各國立法例率皆禁止「蒐集、處理或利用」敏感性個資。[236]英國「資料保護法」(Data Protection Act 1998)禁止「處理」(process)敏感性個資，此規定與「歐盟個資指令」相同，[237]德國「聯邦資料保護法」(Bundesdatenschutzgesetz, BDSG)禁止：公務機關「蒐集」(collection)敏感性個資；[238]私人機構「蒐集」(collection)、「處理」(processing)或「使用」(use)敏感性個資。[239]澳洲「國家隱私原則」(NPPs)第10點禁止私人機構[240]「蒐集」(collection)敏感性個資。[241]

綜上，各國立法例關於禁止敏感性個資之「操作」，有區分「禁止處理」、「禁

---

[235] 參見前揭註 102。

[236] 歐盟會員國都遵循「歐盟個資指令」的處理方式，原則禁止處理敏感性個資，僅於符合例外情況時，始得進行處理。此外，丹麥、德國、希臘、義大利與葡萄牙增加額外規定，認為**處理敏感性個資，須先經主管機關「事前審查」或「事先許可」**參見 Korff, *supra* note 31, at 7.2

[237] 有認為此一法定豁免禁止之清單，為列舉規定者，參見 MORGAN & BOARDMAN, *supra* note 120, at 8.3.1.2

[238] 參見德國聯邦資料保護法 § 13(2)

[239] 參見德國聯邦資料保護法 § 28(6)

[240] 由於 NPPs 僅適用於私人機構，並不適用於公務機關，為免疏漏，「澳洲法改會」建議將其擴大適用至公務機關，參見 1 ALRC, *supra* note 32, Recommendation 22-1 & 25-2 此外，基於將 NPPs 擴張至公務機關之故，為使公務機關便於執行法定職務，「澳洲法改會」建議新增例外得情形：「因法律授權或要求而予以蒐集」以及「為避免他人之生命或健康遭受重大危難」之情況時，得豁免限制而蒐集敏感性個資，參見 Recommendation 22-2 & 22-3.

[241] 參見澳洲隱私法「國家隱私原則」第 10 點。澳洲隱私法(Privacy Act 1988)僅禁止私人機構「蒐集」(collection)敏感性個資，而未禁止「使用或揭露」(Use and Disclosure)敏感性個資。私人機構「使用或揭露」敏感性個資時，須適用「國家隱私原則」第 2 點(NPPs 2)之規定。

止蒐集」或「禁止蒐集、處理或利用」者，我「個資法」係一體禁止公務機關或非公務機關「蒐集、處理或利用」敏感性個資，並未加以區分。本文認為，此規定較部分立法例僅限制蒐集敏感性個資者，涵蓋周延，更能完善保護敏感性個資，值得稱許。

第二節　得「蒐集、處理或利用」之例外

敏感性個資之立法，乃以「禁止蒐集、處理或利用」為原則，例外時（即「豁免」禁止時）始得「蒐集、處理或利用」。我「個資法」第 6 條第 1 項但書規定四種例外情形，以下分述之。

一、法律明文規定者

「個資法」第 6 條第 1 項但書規定：公務機關或非公務機關於「法律明文規定」時，得蒐集、處理或利用同項所列之敏感性個資。

本項所稱之「法律」，依其文義解釋，應限「經立法院三讀通過，總統公布施行之法律」，而不及「行政機關發佈之法規命令」。[242]至於其他法律是否一概優先本法適用，仍有疑義。有關本法與其他法律之關係，「舊個資法」第 2 條規定：「個人資料之保護，依本法之規定。但其他法律另有規定者，依其規定」，惟本條於修正時已遭刪除，立法說明謂：

> **本法之性質應為普通法，其他特別法有關個人資料蒐集或利用之規定，不論較本法規定更為嚴格或寬鬆者**，依特別法優於普通法之法理，**自應優先適用各該特別規定**。惟若無特別規定，當然仍應適用本法，毋庸贅述。且本法修正草案亦有相關例外條款包含「法律明文規定」，足資適用，例如：**第六條第一款**、第十六條第一款、第十九條第一款或第二十條第一項第一款規定。是以，**為避免所謂「特別規定」令人誤解為全面排除本法適用，爰刪除本條規定**。

[242] 類似立法例可參見德國聯邦資料保護法第 13 條第 2 項第 1 款與第 14 條第 5 項。

自上開立法說明觀之，**所謂須「優先適用其他法律」之情形，應限於「其他法律有特別規定（個資之蒐集、處理或利用）者」**（無論寬嚴），[243]**其他法律無特別規定（個資之蒐集、處理或利用）時，仍一律適用「個資法」**。本文認為，為確保「資料控制人蒐集、處理或利用敏感性個資時，所應遵循之保護義務」，不因其他法律漏未規定而被架空，本款所謂優先適用其他法律之情形，應適度限縮於**「其他法律規定公務機關或非公務機關得蒐集、處理或利用敏感性個資」之規定，以排除「個資法」第 6 條第 1 項之限制**，而非謂完全排除適用本法之其他規定，除非「其他法律之規定較（個資法）嚴格」者。

有關「公務機關或非公務機關蒐集、處理或利用敏感性個資」之「法規命令」，雖有母法授權之依據，但其仍不屬本款適用範圍。有關機關不得以「法規命令」適用本款（法律明文規定），蒐集、處理或利用敏感性個資，例如：

1. 人工生殖機構許可辦法第 23 條第 1 項：公益法人之精子保存庫，應「製作」（按：屬個資之「蒐集」）捐贈人之健康檢查紀錄，該精子提供後，紀錄須一併移轉「保存」（按：屬個資之「處理」），並設有保存年限。[244]
2. 學生健康檢查實施辦法第 4 條第 1 項：學校於新生入學時，應「調查」（按：

[243] 立法者所稱：無論寬嚴皆全然放棄「個資法」之規定，是否妥適，仍有待研究。查德國聯邦資料保護法 §1(3)規定：「其他聯邦法律適用於個人資料者，包括公開此類資料，應優先本法（德國聯邦資料保護法）而適用」，同樣將其他法律視為特別法，優先於德國聯邦資料保護法適用，與我「舊個資法」規定相同，惟其但書規定：為「履行『法律上保密』義務或『非法定之職業、國家機密』義務」者，仍須適用德國聯邦資料保護法，無優先適用其他法律之餘地，此規定為我「個資法」所無，可茲參考。

[244] 參照人工生殖機構許可辦法(99/12/02)第 23 條第 1 項：「精子保存庫**應確認**捐贈人已接受健康檢查及評估，並依本法第七條第二項及第九條第二項規定**製作紀錄且妥善保存**，精子提供至醫療機構使用時，該紀錄影本應隨同移轉至醫療機構保存」；第 2 項：「精子保存庫對於前項紀錄，應於精子使用或銷毀後繼續保存七年」。

屬個資之「蒐集」）學生健康基本資料，並做成「紀錄」（按：屬個資之「處理」）。[245]

3. 性侵害加害人檔案資料管理及使用辦法第 5 條第 1 項：司法機關得請警政署刑事警察局「提供」（按：屬個資之「蒐集」）「去氧核醣核酸基因型比對資料」。[246]

以下將「有關公務機關或非公務機關蒐集、處理或利用敏感性個資」之法律，依敏感性個資之類型，分項列舉。

（一）與「醫療、健康檢查」相關之法律

綜觀「個資法」所列之五類敏感性個資，四類與醫療相關。我國有關「公務機關或非公務機關蒐集、處理或利用『醫療、健康檢查』資料」之法律，例如：

1. 人工生殖法第 7 條第 1 項：人工生殖機構應就受術夫妻或捐贈人進行（健康）檢查評估，並製作紀錄，實施人工生殖之醫療機構亦應「製作」（按：屬個資之「處理」）紀錄，並不得提供捐贈人之資料予受術實施人工生殖之夫妻。[247]

---

[245] 參照學生健康檢查辦法(99/10/05)第 4 條第 1 項：「學校辦理新生入學時，應進行學生健康基本資料調查，並做成紀錄…」。

[246] 參照性侵害加害人檔案資料管理及使用辦法(94/12/16)第 5 條第 1 項：「法院、檢察署、軍事法院、軍事法院檢察署、司法、軍法警察機關於偵查或審理案件有必要時，得請內政部性侵害防治委員會提供第二條第一款、第二款及第六款之加害人檔案資料。第二項：「前項機關有利用第二條第三款至第五款檔案資料之必要時，得洽請內政部警政署刑事警察局提供」。

[247] 參照人工生殖法(96/03/21) 第 7 條第 1 項：「人工生殖機構於實施人工生殖或接受捐贈生殖細胞前，應就受術夫妻或捐贈人為下列之檢查及評估：一、一般心理及生理狀況。二、家族疾病史，包括本人、四親等以內血親之遺傳性疾病紀錄。三、有礙生育健康之遺傳性疾病或傳染性疾病。四、其他經主管機關公告之事項」；第 2 項：「前項之檢查及評估，應製作紀錄。」

2. 人體器官移植條例第 11 條第 1 項：醫療機構應將醫療紀錄「記載」（按：屬個資之「處理」）於捐贈者病歷內，受捐贈者之醫療機構並應與受捐贈者之病歷一併「保存」（按：屬個資之「處理」）。[248]
3. 傳染病防治法第 31 條：醫療機構人員應「詢問」（按：屬個資之「蒐集」）病人之相關醫療資訊。[249]
4. 學校衛生法第 9 條：學校應將學生健康檢查之結果，「載入」（按：屬個資之「處理」）學生資料並予保密。[250]
5. 保險法第 126 條：保險人於訂立保險契約前，得對被保險人「施以」（按：屬個資之「蒐集」）健康檢查。[251]

（二）與「基因、性生活」相關之法律

我國有關「公務機關或非公務機關蒐集、處理或利用『基因』資料」之法律，例如：

第 14 條第 1 項：「醫療機構實施人工生殖，**應製作紀錄**，並載明下列事項：一、受術夫妻之姓名、住（居）所、國民身分證統一編號或護照號碼、出生年月日、身高、體重、血型、膚色及髮色。二、捐贈人之國民身分證統一編號或護照號碼及在醫療機構之病歷號碼。三、人工生殖施術情形」；第 2 項：「醫療機構**依受術夫妻要求提供前項病歷**複製本時，**不得包含**前項第二款之資料」。

[248] 參照人體器官移植條例(100/12/21)第 11 條第 1 項：「摘取器官之醫療機構，**應將完整之醫療紀錄記載於捐贈者病歷**，並應善盡醫療及禮俗上必要之注意」；第 2 項：「器官捐贈者所在之醫療機構應於受移植者之醫療機構施行移植手術前，提供捐贈者移植相關書面檢驗報告予受移植者之醫療機構，受移植者之醫療機構並**應併同受移植者之病歷保存**」。

[249] 參照傳染病防治法(98/01/07)第 31 條：「醫療機構人員於病人就診時，**應詢問其病史、就醫紀錄**、接觸史、旅遊史及其他與傳染病有關之事項；病人或其家屬，應據實陳述」。

[250] 參照學校衛生法(91/02/06)第 9 條：「學校**應**將學生**健康檢查**及疾病檢查結果**載入**學生資料，併隨學籍轉移。前項學生資料，**應予保密**，不得無故洩漏。但應教學、輔導、醫療之需要，經學生家長同意或依其他法律規定應予提供者，不在此限」。

[251] 參照保險法(100/11/30)第 126 條。

1. 去氧核醣核酸採樣條例第 5 條：特定犯罪之被告或犯罪嫌疑人，應接受去氧核醣核酸之「強制採樣」（按：屬個資之「蒐集」）。[252]
2. 人體生物資料庫管理條例第 6 條：設有人體生物資料庫之機構，得經當事人同意後，進行「生物檢體」之「採集」（按：屬個資之「蒐集」）。[253]

所謂「生物檢體」僅限「指自人體採集之細胞、組織、器官、體液或經實驗操作所產生，足以辨識參與者生物特徵之衍生物質」[254]，表面上「生物檢體」似非「個資法」第 6 條第 1 項所列之敏感性個資，惟細譯其內容，可知設有人體生物資料庫之機構尚得自「生物檢體」中獲得參與者之「基因」資料。[255]依「個資法」第 6 條第 1 項，「基因」為敏感性個資，故設有人體生物資料庫之機構，自應適用本款規定以「採集」「生物檢體」資料。[256]

所謂「性生活」之資料，通常指記載「性傾向」(sexual orientation)或「性行為」(sexual practices)之資料。[257]我國目前並無規定「公務機關或非公務機關蒐集、處理或利用『性生活』資料」之法規，惟「性生活」資料仍有可能於「公務機關執行法定職務或非公務機關履行法定義務」時「直接」或「附帶」蒐集取得，詳見本節後「公務機關執行法定職務或非公務機關履行法定義務」之討論。

---

[252] 參照去氧核醣核酸採樣條例(101/01/04)第 5 條。有學者認為本條規定之「強制採樣要件」過於寬鬆，參見劉靜怡，〈DNA 採樣、犯罪預防和人權保障〉，《台灣法學》，124 期，頁 122（2009 年 3 月）。

[253] 參照人體生物資料庫管理條例(100/01/26)第 6 條。

[254] 人體生物資料庫管理條例(100/01/26)第 3 條第 1 款。

[255] 參照人體生物資料庫管理條例(100/01/26)第 7 條第 8 款。

[256] 人體生物資料庫管理條例草案原增列排除適用「舊個資法」之規定，後已刪除，參見顏上詠，〈台灣人體生物資料庫管理條例草案評析〉，《月旦法學雜誌》，168 期，頁 159（2009 年 5 月）。

[257] 參照「個資法」修正說明；澳洲隱私法 §6(1).

（三）與「犯罪前科」相關之法規

我國有關「公務機關或非公務機關蒐集、處理或利用『犯罪前科』資料」之法律，例如：

1. 性侵害犯罪防治法第 9 條：中央主管機關應「建立」包括犯罪資料、指紋、去氧核醣核酸紀錄等之全國性侵害加害人檔案資料。[258]
2. 性別平等教育法第 27 條：學校應「查閱」任用人員有無性侵害之犯罪記錄。[259]

3. 警察刑事紀錄證明核發條例第 3 條：警察機關依司法或軍法機關判決確定、執行之刑事案件資料，可「作成紀錄證明」(按：屬個資之「處理」)。[260]

[258] 參照性侵害犯罪防治法(100/11/09)第 9 條：「中央主管機關**應建立**全國性侵害加害人之**檔案資料**；其內容應包含姓名、性別、出生年月日、國民身分證統一編號、住居所、相片、**犯罪資料**、**指紋**、**去氧核醣核酸紀錄**等資料」。

[259] 參照性別平等教育法(100/06/22)第 27 條：「學校任用教育人員或進用其他專職、兼職人員前，**應依性侵害犯罪防治法之規定，查閱其有無性侵害之犯罪紀錄**，或曾經主管機關或學校性別平等教育委員會調查有性侵害、性騷擾或性霸凌行為屬實並經該管主管機關核准解聘或不續聘者」。近日教育部擬具「不適任教育人員之通報與資訊蒐集及查詢辦法」建立「全國不適任教師查詢系統」，以供各級學校履行教育人員任用條例(100/11/30)第 26 條、第 30 條所定之法定職務，並查詢有無同法第 31 條第 1 項不適任教師之事由（特定犯罪前科）。**此類情形雖非屬法律明文規定得蒐集敏感性個資之情形，但仍屬公務機關執行職務之範圍**，可適用「個資法」第 6 條第 1 項但書第 2 款（「公務機關執行法定職務或非公務機關履行法定義務所必要者」）之情形，參見教育部 100 年 4 月 29 日臺人（二）字第 1000057150 號函。

[260] 參照警察刑事紀錄證明核發條例(91/06/12)第 3 條：「本條例所稱警察刑事紀錄證明，係指警察機關**依司法或軍法機關判決確定、執行之刑事案件資料所作成之紀錄證明**」。

二、公務機關執行法定職務或非公務機關履行法定義務所必要者

「個資法」第 6 條第 1 項但書第 2 款規定：「公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施」時，得蒐集、處理及利用敏感性個資。本款規定與前款「法律明文規定」有相當程度之競合。蓋公務機關之「法定職務」或非公務機關之「法定義務」仍屬「法律明文規定」之事項，[261]如法律僅明定該機關之職務或義務，而**未規定公務機關或非公務機關得進行「蒐集、處理或利用敏感性個資」**之行為，而**公務機關或非公務機關為了執行法定義務或履行法定職務所必要，需要「蒐集、處理或利用」敏感性個資，應適用本款**豁免禁止規定。以下分項討論本款要件。

（一）公務機關執行法定職務

所謂「公務機關」係指**依法行使公權力**之中央或地方機關或行政法人。[262]該**機關須依（組織）法或命令設立**，[263]且「機關」並不限於行政機關，尚包括司法機關、立法機關及軍事機關。[264]所謂「法定職務」係指「**行使職務上權力或履行**

---

[261] 惟此一區分方法並無太多實益，蓋執行法定職務或履行法定義務，豈非「法律明文規定」？故本文建議修正刪除此項，直接適用「法律明文規定者」豁免禁止即可。

[262] 參照「個資法」第 2 條第 8 款與中央行政機關組織基準法(99/02/03)第 3 條：「機關乃就法定事務，有決定並表示國家意思於外部，而依組織法律或命令設立，行使公權力之組織」。

農會與國營企業是否為「個資法」上之公務機關，實務上持否定態度，參見法務部 99 年 4 月 15 日法律字第 0999004810 號函與法務部 86 年 3 月 8 日法律決字第 08574 號函。

「公權力」之定義，一般指「私經濟作用以外之其他公法行為」，參見葉百修，〈國家賠償法〉，翁岳生主編，《行政法二〇〇〇》，頁 1357-1365（2000 年修訂二版）。

[263] 構成機關之要件為：具有單獨之組織法規、獨立編制及預算、有印信，否則屬於內部單位，無法對其提起行政救濟，參見吳庚，《行政法之理論與實用》，頁 178（2005 年增訂九版）。

[264] 「舊個資法」時期之解釋函令即將「軍事機關」視為公務機關，參照法務部 90 年 4 月 19 日法律字第 000178 號函。

其職務上義務，而與其所執掌之公務有關」[265]，此「法定」不限「經立法院三讀通過，總統公布施行者」者，「法規命令」亦有其之適用。[266]明白掌握公務機關之定義，將有助於當事人因資料遭不法蒐集、處理及利用，而請求賠償。

我國有關「公務機關因執行法定職務而需要蒐集、處理或利用敏感性個資」之「法律」，例如：

1. 人類免疫缺乏病毒傳染防治及感染者權益保障條例第 15 條：主管機關應通知，曾與感染者發生性行為之人至醫療機構檢查。[267]
2. 身心障礙者權益保障法第 21 條：各地主管機關應舉辦身心障礙者健康檢查。[268]
3. 社會秩序維護法第 91 之 1 條第 1 項：縣市政府於制定有關性交易之自治條例內，須包含性交易者應接受健康檢查之規定，該場所負責人亦應督促其接受健康檢查。[269]

---

[265] 此意義係參考國家賠償法之規定，蓋根據「個資法」第 31 條，向公務機關請求損害賠償，應適用國家賠償法。

[266] 參見葉百修，前揭（註 262）文，頁 1354。

[267] 人類免疫缺乏病毒傳染防治及感染者權益保障條例(96/07/11)第 15 條：「主管機關**應通知**下列之人，至指定之醫事機構，**接受**人類免疫缺乏病毒諮詢與**檢查**：…二、與感染者發生危險性行為、共用針具、稀釋液、容器或有其他危險行為者」。

[268] 身心障礙者權益保障法(100/06/29)第 21 條：「直轄市、縣（市）主管機關**應定期舉辦身心障礙者健康檢查及保健服務**，並依健康檢查結果及身心障礙者意願，提供追蹤服務。前項保健服務、追蹤服務、健康檢查項目及方式之準則，由中央衛生主管機關會同中央主管機關定之」。

[269] 參照社會秩序維護法(100/11/04)第 91-1 條第 1 項：「直轄市、縣（市）政府得因地制宜，制定自治條例，規劃得從事性交易之區域及其管理；第 2 項：「前項自治條例，應包含下列各款規定：…七、性交易服務者，**應**辦理登記及申請證照，並定期**接受健康檢查**。性交易場所負責人，亦**應負責督促其**場所內之性交易服務者定期**接受健康檢查**」。

4. 勞工保險條例第 28 條：保險人（勞保局）審議爭議案件且必要時，得要求醫療機構提出報告或調閱病歷。[270]
5. 全民健康保險法第 80 條第 1 項：主管機關為審議保險爭議事項或保險人為辦理各項保險業務時，得要求醫療機構提出報告或調閱病歷。[271]
6. 性別平等教育法第 14 條第 2 項：學校應對「因性傾向而處於不利狀態」之學生提供協助。[272]
7. 民法第 1094 之 1 條：法院選定或改定監護人時，應注意監護人之「健康情形」與「前科紀錄」。[273]
8. 統計法第 3 條：政府機關得辦理基本國勢調查（人口普查）。[274]

通常辦理人口普查通常須登記「人口基本特徵」、「國人健康狀況」等，[275]此

---

[270] 參照勞工保險條例(100/04/27)第 28 條：「保險人為審核保險給付或勞工保險監理委員會**爲審議爭議案件認有必要者**，得向被保險人、受益人、投保單位、各該醫院、診所或領有執業執照之醫師、助產士等**要求提出報告**，或**調閱**各該醫院、診所及投保單位之**病歷**、薪資帳冊、檢查化驗紀錄或放射線診斷攝影片（X 光照片）及其他有關文件，被保險人、受益人、投保單位、各該醫院、診所及領有執業執照之醫師或助產士等均不得拒絕」。

[271] 參照全民健康保險法(100/06/29)第 80 條第 1 項：「主管機關**爲審議保險爭議事項**或保險人**爲辦理各項保險業務**，得請**保險對象**、**投保單位**、**扣費義務人及保險醫事服務機構提供**所需之帳冊、簿據、**病歷**、**診療紀錄**、醫療費用成本等文件或有關資料，或對其訪查、查詢。保險對象、投保單位、扣費義務人及保險醫事服務機構不得規避、拒絕、妨礙或作虛偽之證明、報告或陳述」。

[272] 參照性別平等教育法(100/06/22)第 14 條第 2 項：「學校應對因**性別**、**性別特質**、**性別認同或性傾向**而處於不利處境之學生積極提供協助，以改善其處境」。

[273] 參照民法(99/05/26)第 1094 之 1 條：「法院選定或改定監護人時，應依受監護人之最佳利益，審酌一切情狀，尤應注意下列事項：一、受監護人之年齡、性別、意願、健康情形及人格發展需要。二、監護人之年齡、職業、品行、意願、態度、**健康情形**、經濟能力、生活狀況及有無犯罪**前科紀錄**…」。

[274] 參照統計法(61/05/26)第 3 條、統計法施行細則(88/09/15)第 7 條。

[275] 參照行政院院臺財字第 0980052517 號函。

類資料有可能屬於敏感性個資，[276]公務機關蒐集、處理或利用該資料應注意本法規定。

我國有關「公務機關因執行法定職務而需要蒐集、處理或利用敏感性個資」之「法規命令」，例如：

1. 職業災害勞工保護法個資法施行細則第 17 條：勞保局審核勞工是否遭遇職業疾病，必要得通知勞工或事業單位檢送健康檢查紀錄等資料。[277]
2. 老人健康檢查保健服務及追蹤服務準則第 2 條：各縣市主管機關應定期辦理老人健康檢查。[278]
3. 身心障礙者健康檢查及保健服務準則第 2 條：各縣市主管機關應協助身心障礙團體進行健康檢查或保健服務。[279]
4. 優生保健法個資法施行細則第 2 條：主管機關得辦理包含「基因」項目

[276] 比較法上，人口普查蒐集之資料通常是「種族」統計，或「國籍」、「語言」等事項，惟種族資料於我國非屬敏感性個資，**適用上僅須注意「健康資料」即可**。有關種族統計資料之處理，參見 Study Report of the European Commission against Racism and Intolerance on "Ethnic" statistics and data protection in the Council of Europe countries, at 24 (Oct. 10, 2007), *available at* http://www.coe.int/t/dghl/monitoring/ecri/activities/themes/Ethnic_statistics_and_data_protection.pdf

[277] 參照職業災害勞工保護法施行細則(91/04/26)第 17 條：「勞保局依本法第六條第一項、第八條第一項、第二項、第九條第一項及第二十條規定審核勞工是否遭遇職業疾病，**必要時得通知**勞工或事業單位**檢送**勞工職業疾病診斷書、既往之作業經歷、職業暴露資料、體格及**健康檢查紀錄**、**病歷**、生活史及家族病史等資料」。

[278] 參照老人健康檢查保健服務及追蹤服務準則(96/07/31)第 2 條：「直轄市、縣（市）主管機關**應定期舉辦老人健康檢查及保健服務**，並應以書面或公告方式通知檢查時間及地點」。

[279] 參照身心障礙者健康檢查及保健服務準則(97/01/22)第 2 條：「直轄市、縣（市）主管機關**舉辦身心障礙者健康檢查**及保健服務，應以書面或公告通知檢查時間及地點，副知轄內相關身心障礙團體；並視實際需要**協助就檢**」。

之人民健康或婚前檢查。[280]

以上皆屬於公務機關之法定職務「直接」蒐集、處理或利用敏感性個資之情形，惟法定職務種類複雜，就立法技術而言，實難將各公務機關之職務與權限（內應處理之個人資料），鉅細靡遺詳細規範於各該法規，特別是負有調查或情報蒐集任務之機關。[281]所以公務機關仍有可能於執行一般公務時，「附帶（間接）」蒐集、處理或利用敏感性個資，例如法院宣判之判決、法院審判中之紀錄、警察機關記載之筆錄、情報機關蒐集之資料等。

有關訴訟程序中之敏感性個資，各訴訟法並未對此有明確規範，僅消極規定內容涉及當事人隱私者，法院得拒絕公開資料或拒絕提供閱覽。[282]紐西蘭「法律委員會」(New Zealand Law Commission)建議制定「法院資訊保護法」(Court Information Act)，限制公開孩童或無行為能力人之敏感性及隱私資料，係特別針對敏感性個資所為之限制，可茲參考。[283]此外，關於警察機關或情報機關因執行法定職務（與敏感性個資無關之職務），而「附帶」蒐集、處理或利用之敏感性個資，例如警察依法蒐集資料，[284]此時應許該機關適用本款規定，豁免禁止而蒐集、處

---

[280] 參照優生保健法施行細則(101/04/05)第 2 條：本法第六條所稱健康或婚前檢查，其項目如附件一…三、遺傳性疾病檢查 (一) 家族疾病史問診。 (二) 染色體、基因、生化檢驗」。

[281] *See* 2 AUSTRALIAN LAW REFORM COMMISSION, FOR YOUR INFORMATION: AUSTRALIAN PRIVACY LAW AND PRACTICE 37.102 & 37.108 (2008).

[282] 參見民事訴訟法第 195-1 條（不公開審判）、第 242 條第 3 項（拒絕閱覽訴訟卷宗）與第 344 條（豁免當事人提出書證）；刑事訴訟法第 33 條第 2 項（拒絕辯護人檢閱卷宗等）；類似規定亦存在於行政程序法第 46 條第 3 款（拒絕當事人卷宗閱覽）。其他法規仍有應予保密不公開案件之規定，參見李惠宗，〈判決書上網公開與個人資訊自決權的衝突〉，《月旦法學雜誌》，154 期，頁 21-34（2008 年 3 月）。

[283] New Zealand Law Commission, Access to Court Records, Report 93 (2006), rec R6.

[284] 參見警察職權行使法(100/04/27)第 11 條與第 12 條。

理或利用敏感性個資。[285]

（二）非公務機關履行法定義務

「非公務機關」指**公務機關以外之自然人、法人或其他團體**。[286]我國於「舊個資法」時期，因對「非公務機關」之定義係採列舉方式規定，[287]自然人及部分法人團體皆排除適用，對個人資料之保護似嫌不足。2011 年新修正之「個資法」則摒棄上述定義，將「公務機關以外之機構或個人」皆視為「非公務機關」，擴大「個資法」之適用範圍，值得稱許。所謂「法定義務」應指「非公務機關」為履行「法律規定」或「法律明確授權」之事項。至於非公務機關係以完全履行公共管理為目的者，則應視為公務機關。[288]

我國「法律」規定有關「非公務機關履行法定義務」而需要蒐集、處理或利用敏感性個資者，例如：

---

[285] 比較法上尚存在「基於當事人訴訟或行使法律權利」而豁免禁止之情形，惟我「個資法」並未規定此要件，本節後詳。

[286] 參照「個資法」第 2 條第 8 款。

[287] 參照「舊個資法」第 3 條第 7 款，非公務機關包括：「徵信業及以蒐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、保險業及大眾傳播業；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」。實務上認為「大廈管理委員會」（法務部 99 年 1 月 21 日法律字第 099070043 號函）、「議員服務處」（法務部 97 年 10 月 31 日法律字第 0970037059 號函）、「財團法人保險犯罪防制中心」（法務部 94 年 10 月 5 日法律字第 0940033240 號函）、「人力資源服務網站」（法務部 89 年 6 月 28 日法律字第 020741 號函）、「中華民國聾啞資源協會」（法務部 85 年 10 月 16 日法律決字第 26516 號函）不屬「舊個資法」所稱之「非公務機關」。

[288] 參見「個資法」第 4 條，比較法例可參見德國聯邦資料保護法 §2(4)。機關如將公權力委託私人機構行使，須有法規依據，參見湯德宗，〈行政程序法之適用〉，《行政程序法論》，頁 133（2003 年）。

1. 游離輻射防護法第 16 條第 1 項：雇主應要求工作人員進行健康檢查，該紀錄並應予保存。[289]
2. 核子反應器設施管制法第 12 條：經營者應定期辦理健康檢查。[290]
3. 勞工安全衛生法第 12 條第 1 項：雇主對在職勞工應定期施行健康檢查，該紀錄同樣應予保存。[291]
4. 船員法第 8 條第 1 項：船員應經健康檢查，該紀錄並應予保存。[292]
5. 傳染病防治法第 39 條第 1 項：醫師發現傳染病應通報當地主管機關。[293]
6. 幼兒教育及照顧法第 31 條第 1 項：幼兒園應協助辦理幼兒健康檢查，且應將該結果載入（按：屬個資之「處理」）幼兒健康資料檔案，並妥善管理「保存」（按：屬個資之「處理」）。[294]

---

[289] 參照游離輻射防護法(91/01/30)第 16 條第 1 項：「雇主僱用輻射工作人員時，**應要求其實施體格檢查**；對在職之輻射工作人員應實施定期健康檢查，並依檢查結果為適當之處理」；第 5 項：「第一項體格檢查、**健康檢查**及第二項特別醫務監護之**紀錄**，雇主**應依主管機關之規定保存**」。

[290] 參照核子反應器設施管制法(92/01/15)第 12 條：「經營者**應定期辦理**所屬核子反應器運轉人員**健康檢查**，身心狀況不適宜繼續擔任運轉工作者，應停止之；必要時，主管機關亦得令經營者予以停止」。

[291] 參照勞工安全衛生法(91/06/12)第 12 條第 1 項：「雇主於僱用勞工時，**應施行體格檢查**；對在職勞工應施行定期健康檢查；對於從事特別危害健康之作業者，應定期施行特定項目之健康檢查；並建立健康檢查手冊，發給勞工；第 2 項：「前項檢查應由醫療機構或本事業單位設置之醫療衛生單位之醫師為之；**檢查紀錄應予保**存；健康檢查費用由雇主負擔；第 3 項：「前二項有關體格檢查、健康檢查之項目、期限、紀錄保存及健康檢查手冊與醫療機構條件等，由中央主管機關定之」。

[292] 參照船員法(100/06/29)第 8 條第 1 項：「船員**應經體格檢查合格**，並依規定領有船員服務手冊，始得在船上服務」；第 2 項：「已在船上服務之船員，應接受定期健康檢查；經檢查不合格或拒不接受檢查者，不得在船上服務」；第 3 項：「船員體格檢查及健康檢查，應由符合規定條件之醫療機構或本事業單位所設置醫療單位為之；其**檢查記錄應予保存**」。

[293] 參照傳染病防治法(98/01/07)第 39 條第 1 項：「醫師診治病人或醫師、法醫師檢驗屍體，發現傳染病或疑似傳染病時，**應立即採行必要之感染控制措施，並報告當地主管機關**」。

[294] 參照幼兒教育及照顧法(100/06/29)第 31 條第 1 項：「建立幼兒健康管理制度。直轄市、縣（市）

值得注意，上開幼兒園處理幼兒健康檢查資料之情形，將同時符合「個資法」第 6 條第 1 項但書第 1 款「法律明文規定」（應將結果載入檔案）與第 6 條第 1 項但書第 2 款「非公務機關履行法定義務」（應予協助辦理）之情況。本文認為，各款規定之目的在於免除第 6 條第 1 項所定之限制，故為避免徒增適用疑義，公務機關或非公務機關於符合多款例外（得蒐集、處理或利用敏感性個資）之情形時，僅須擇一適用即可。

（三）「必要」

依我「個資法」第 6 條第 1 項，公務機關或非公務機關，於執行法定職務或履行法定義務所「必要」，且「有適當安全維護措施」者，得蒐集、處理或利用敏感性個資。[295]所謂「必要」，查我「個資法」與「個資法施行細則草案」並未規定，本文參考英國資料保護官署(The Information Commissioner's Office, ICO)所提供之指南，認為資料管理人應考量：**其處理之目的是否合法、處理該個人資料是否為唯一達成該目的之手段、其處理與追求之目的須不得顯失均衡**。[296]其意義殆與憲法上所謂「比例原則」相當。[297]

衛生主管機關辦理幼兒健康檢查時，幼兒園**應予協助**，並依檢查結果，施予健康指導或轉介治療；第 2 項：「幼兒園**應將幼兒健康檢查、疾病檢查結果**、轉介治療及預防接種等資料，**載入**幼兒健康資料檔案，並妥善管理及保存」；第 3 項：「幼兒園、教保服務人員及其他人員對**前項幼兒資料應予保密**。但經家長同意或依其他法律規定應予提供者，不在此限」。

[295] 此用語原先並未出現於「個資法」草案中，而於立院二讀協商時始加入條文中，參見立法院公報，99 卷 26 期，頁 67（2010 年 4 月）。

[296] UK Information Commissioner, *supra* note 44, para. 3.1.6; MORGAN & BOARDMAN, *supra* note 120, at 8.3.4.1.

[297] 參見湯德宗，〈違憲審查基準體系建構初探--「階層式比例原則」構想〉，廖福特主編，《憲法解釋之理論與實務》，第六輯（下冊），頁 597-599（2009 年）。

（四）「適當安全措施」

按「個資法」並未定義「適當安全措施」,「個資法施行細則草案」第 9 條第 1 項，增列「適當安全維護措施、安全維護事項或適當之安全措施」之定義，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必要措施**。[298]同條第 2 項並就「必要措施」之內容詳細規範。[299]

上開有關「公務機關或非公務機關執行法定職務或履行法定義務」之法規中，僅部分規定該機關或機構應將蒐集得來之（健康）資料予以保存，而未規定該公務機關或非公務機關應建立適當安全措施。本文建議，將來上開法規應適度修正，以確實符合「個資法」之要求。此外，「個資法」第 18 條（公務機關）與第 27 條（非公務機關），本來就規定公務機關或非公務機關保有個人資料時，應辦理安全維護事項（公務機關）或採行適當安全措施（非公務機關），即便前開法規未規定「適當安全維護措施」，公務機關或非公務機關仍然須履行上開義務，須提供「適當安全維護措施」。

三、當事人自行公開或其他已合法公開者

「個資法」規定第三種得豁免禁止，而蒐集、處理及利用敏感性個資之情形為「資料經當事人自行公開或其他已合法公開」者。蓋資料若在自願或是合法公開的情況下公諸於世，資料主體（本人）之隱私應不會受到侵害，除非該資料涉

[298] Directive 95/46/EC Art. 17(1)

[299] 參照「個資法施行細則草案」第 9 條第 2 項：「前項必要措施，應包括下列事項：一、成立管理組織，配置相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、必要之使用紀錄、軌跡資料及證據之保存。十一、個人資料安全維護之整體持續改善」。

及他人，否則應無強制保護之必要。[300]

（一）「當事人自行公開敏感性個資」者

所謂「當事人自行公開」，按「個資法施行細則草案」第 10 條第 1 項規定，當事人自行公開係指**當事人自行對不特定人或特定多數人為揭露**。所謂「公開」，須由資料主體（本人）公開，如該資料係由「第三人」公開，已有侵害本人隱私之虞，自不得藉此豁免禁止。比較立法例，有相同規定，例如「歐盟個資指令」第 8 條第 2 項e款規定，資料顯然經資料當事人公開，或為成立、行使或防禦其法律上之主張所必要者，得豁免處理。此公開須為顯然經深思熟慮後而為過的公開。[301]

（二）「其他已合法公開敏感性個資」者

所謂「其他已合法公開者」，按「個資法個資法施行細則草案」第 10 條第 2 項規定，係指**依法規公示、公告或以其他合法方式公開**之個人資料，例如依「政府資訊公開法」主動或被動公開之資料。[302]查英國資料保護法並未將「依法公開之資料」列為豁免禁止，得蒐集、處理或利用敏感性個資之例外情形。「依法公開之資料」僅豁免適用部分「個人資料保護原則」，例如本人無法要求資料控制人刪

---

[300] 蓋當事人自行公開僅免除「個資法」第 6 條第 1 項前段之限制。以「歐盟個資指令」而言，當事人之自行公開應採高標認定。義大利資料主管機關認為雖然 e-mail 非常容易蒐集，但除非得到 e-mail 收件人的同意，否則不得據以寄送廣告郵件。他們同時也認為，參與網路討論群組並不當然使使用者之電子郵件位置「公開」。法國法院認為，從網路空間蒐集那些非以公開為目的之電子郵件，違反個資法參見 KUNER, *supra* note 34, at 2.79

[301] 參見德國聯邦資料保護法 §§ 13(2)4 & 28(6)3; 英國資料保護法 Sche.3 5; 芬蘭規定其公開者，須限於「資料主體意圖使其公開之敏感性個資」，丹麥與法國規定僅須「主體公開」，而非「顯露」公開，英國與愛爾蘭則規定須「資料主體審慎考慮予以公開之結果」。

[302] 該資料須不具豁免公開之情形，參照「政府資訊公開法」第 18 條。

除、銷毀、封鎖該資料（個人參與原則）；資料控制人無須適時更新該資料（資料品質原則）等。[303]本文認為，公務機關或非公務機關適用本款時應予適度限縮，將公務機關或非公務機關**「合法公開」之行為視為個人資料之「利用」**。[304]公務機關或非公務機關於公開個人資料前，應踐行「通知義務」，並許本人得更正「未經公開」之資訊。[305]

四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序者

「個資法」第 6 條第 1 項第 4 款規定「**公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序**」，得蒐集、處理及利用敏感性個資。本款之主體限公務機關或學術研究機構。所謂「公務機關」係指**依法行使公權力之中央或地方機關或行政法人**；[306]至於「學術研究機構」之定義，「個資法」及「個資法施行細則草案」則未見說明。根據「舊個資法」第 26 條第 2 項（中央目的事業主管機關得發佈非公務機關之收費標準）定頒之「私立學校及學術研究機構製給個人資料複製本收費標準」(100/11/25)第 2 條規定，學術研究機構係指依「學術研究機構設立辦法」核准設立之私立學術研究機構，而根據「學術研究機構設立辦法」，係指**國立研究院及公私立大學研究所以外之學術**

---

[303] 英國資料保護法 §34

[304] 此舉與通說將「資料匿名化」過程視為「資料處理」之原理相同。蓋資料控制人於處理（進行匿名化）資料時，仍須符合個資法相關規定，並無得豁免適用個資法之餘地，參見 Rouillé-Mirza & Wright, *supra* note 133, at 145.

[305] 本文以為，**資訊一旦公開即覆水難收，是否仍須賦予當事人更正權，則有待衡量**，惟「個資法」對此並未區分，當事人仍得根據「個資法」第 11 條向公務機關或私人機構請求更正或停止利用，該資料控制人並負有損害賠償責任。

[306] 參照「個資法」第 2 條第 8 款。詳細討論參見本節第二點。

研究機構，[307]惟此一定義是否可直接適用於「個資法」，尚有疑問。蓋上開定義排除中央研究院、大學研究所等學術研究機構，且中央研究院等各研究機構在定義上又不屬於「個資法」第 2 條第 7 款定義之「公務機關」（須依法行使公權力），故使中央研究院等學術研究機構將無法適用本款以蒐集、處理或利用敏感性個資。本文認為，上開「學術研究機構設立辦法」之目的在於鼓勵私人學術研究之發展，故教育部將學術研究機構之定義排除國立研究院與公私立大學研究所，而「個資法」本條之目的在於「**基於資料之合理利用，促進學術研究發展**」，故定義學術研究機構時，無須排除國立研究院與公私立大學研究所，應認「學術研究機構」係指「**國立研究院、公私立大學與其他公私立學術研究機構**」較為妥適。

公務機關或學術研究機構適用本款以蒐集、處理或利用敏感性個資時，其目的須限於「醫療」、「衛生」或「犯罪預防」三者之一，惟本款後句又規定該蒐集、處理或利用敏感性個資之行為，須「**為**統計或學術研究而有必要」，形同在前項「醫療、衛生或犯罪預防」之目的外，又新增「統計或學術研究而有必要」之目的，故本文認為，公務機關或學術研究機構蒐集、處理或利用敏感性個資，其目的須為：「醫療、衛生或犯罪預防」與「為統計或學術研究而有必要」。

所謂「統計」或「學術研究」，查遍我國法規中並未就此定義，各國立法例普遍將「統計、學術研究」視為「科學研究」(scientific research)之概念，[308]例如德

---

[307] 參照「學術研究機構設立辦法」(97/11/14)第 2 條。

[308] 「歐盟個資指令」並未規範敏感性個資之「醫學研究豁免」，而僅賦予醫療機構得處理敏感性個資之權利（後詳）。一般而言，「醫學研究」通常指「傳染病學」(epidemiology)、「藥物安全監視」(pharmacovigilance)及「臨床實驗」(clinical trial)上對於醫學或健康資料之使用，參見 Stefaan Callens, *The Privacy Directive and Use of Medical Data for Research Purposes*, 2 EURO. J. HEALTH L. 309, 325 (1995).

依據「歐盟個資指令」進行醫學研究，可透過部分條文豁免，例如第 8 條第 2 項 a 款之「當事

國規定公務機關「以科學研究為目的而必要，且執行該研究計畫所得之科學利益，大於當事人於蒐集資料中之利益，同時該研究之目的無法以其他方式實踐，或透過其他方式所費不貲者」[309]得蒐集敏感性個資。奧地利規定「以科學研究或統計之目的」，並針對該目的有詳細規範者，得蒐集敏感性個資。[310]英國定義「研究目的」包含統計與歷史目的。[311]綜上，我「個資法」不妨參照上開立法例，將「統計或學術研究」改以「科學研究」用語代替，修正為：「為科學研究而有必要」。

所謂「一定程序」，「個資法」與「個資法施行細則草案」並未明確規定。「個資法」之修正說明謂：係指當事人資料經過**匿名化處理**，或**依其揭露方式無從再識別特定當事人**者。所謂「依其揭露方式無從識別特定當事人」，依「個資法施行細則草案」第 14 條規定，係指個人資料**以代碼、匿名或其他揭露方式，無從辨識**

人同意」、c 款之「為保護當事人之重大利益」、第 3 項「健康照護目的」、第 4 項「重大公益」等，及第 6 條第 1 項 b 款（基於科學目的之二次利用）、第 6 條第 1 項 e 款（基於科學目的得延長保存期限）等，詳細參見 Herman Nys, *The Scope of Exemptions for Medical Research*, *in* THE DATA PROTECTION DIRECTIVE AND MEDICAL RESEARCH ACROSS EUROPE 51-55 (Deryck Beyleveld et al. eds., 2004).

丹麥規定進行任何與敏感性個資相關之研究，須通知資料保護機關(Data Surveillance Authority)，參見 Mary Rosenzweig & Lisbeth Kundsen, *Research Ethics Committees in Denmark*, *in* Research Ethics Committees, Data Protection and Medical Research in European Countries 37 (2005). 有學者以為，在未經當事人同意下，以研究目的交換醫療資料，將有違必要性原則，參見 Stefaan Callens, *The Privacy Directive and Use of Medical Data for Research Purposes*, 2 EURO. J. HEALTH L. 325 (1995).

[309] 德國聯邦資料保護法 § 13(2)(8)

[310] 奧地利資料保護法 §§ 9(10) & 46. 此外，奧地利規定，敏感性個資具有統計可能性(statistical probability)時，將不屬敏感性個資(§ 4(2))，例如以家族姓氏來識別種族或宗教背景，參見 Helmut Ofner, *Data Protection in Austria*, *in* IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE IN RELATION TO MEDICAL RESEARCH IN EUROPE 13 (Deryck Beyleveld et al. eds., 2004).

[311] 以科學研究為目的之資料，排除適用部分個人資料保護原則，參見英國資料保護法 § 33(4)

該特定個人，或需費過鉅或耗時過久始能予以辨識者。[312]本文建議，為確保本款所適用之資料無法識別特定當事人，且有助於「個資法」之用語統一與概念理解，修法將「一定程序」之用語改為「經匿名化處理或依其揭露方式無從識別特定本人者」。此外，「醫療資料」如經匿名化後，將無法進行科學研究時，依「歐盟執委會」(European Commission)之建議，應免於將該資料進行匿名化處理，[313]故，本文建議本款後段應增列但書「但資料經匿名化處理後無法進行研究者除外」，以合理促進學術研究。又，「個資法」第 6 條第 2 項規定中央目的事業主管機關應會同法務部，就本項之適用範圍、程序及其他遵行事項，訂定辦法。

五、其他

各國立法例對於得蒐集、處理或利用敏感性個資之例外規範數種不同情形，例如「歐盟個資指令」規範 8 種，德國聯邦資料保護法規定 9 種，英國資料保護法規定 10 種。相較我「個資法」僅訂有 4 種得蒐集、處理或利用敏感性個資之情形，我「個資法」規定之例外情形似有不足。以下參照各國立法例，針對我「個資法」不足之處，分項討論。

（一）「經當事人書面知情同意」者

我「個資法」未規定：公務機關或非公務機關「經當事人同意」後，得蒐集、處理或利用敏感性個資。其實，「個資法」草案，原先訂有「法律未明文禁止蒐集、

312 匿名化之定義，可參見德國聯邦資料保護法 § 3(6)

313 *See* Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data Principle 12.1; Casabona, *supra* note 34, at 41-42. 此見解似並不禁止以醫學研究為目的，處理敏感性個資，參見 Ségolène Rouillé-Mirza & Jessica Wright, *Comparative Study on the Implementation and Effect of Directive 95/46/EC on Data Protection in Europe: Medical Research*, *in* THE DATA PROTECTION DIRECTIVE AND MEDICAL RESEARCH ACROSS EUROPE 213 (Deryck Beyleveld et al. eds., 2004).

處理或利用，且經當事人書面同意」之條款，惟本項於立院審議時遭到刪除，使我「個資法」成為罕見未具「當事人同意」豁免之立法例。「歐盟個資指令」第 8 條第 2 項規定，資料主體「明示同意」(explicit consent)時，得處理敏感性個資；[314]英國資料保護法規定，資料主體「明示同意」(explicit consent)時，得處理敏感性個資；[315]德國聯邦資料保護法規定，資料主體依據第 4a條表達明確同意(expressly consent)，得蒐集敏感性個資。[316]

按敏感性個資之禁止蒐集、處理及利用，係避免該資料之蒐集、處理或利用對當事人之隱私造成侵害，當事人若認為其隱私並無受到侵害之虞，而自願（同意）將其敏感性個資提供予公務機關或非公務機關進行蒐集、處理及利用，原則上似無禁止之理。[317]本文建議「個資法」增列「當事人同意」條款，規定「經當事人書面同意」時，得蒐集、處理或利用敏感性個資。至於是否將「當事人書面同意」列為強制要件，亦即要求公務機關或非公務機關蒐集、處理或利用敏感性個資時，一定要獲得當事人同意，[318]以防資料控制人直接適用其他例外情形，而

---

[314] 本項但書規定：除非各會員國規定「雖經資料主體之同意，仍禁止處理其敏感性個資」。

[315] 英國資料保護法 Sche.3 1.

[316] 德國聯邦資料保護法 §13(2)2.

[317] 此與作為個人資料保護之核心概念之個人資訊自主權(informational self-determination)概念上相同，參見 Antoinette Rouvroy & Yves Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, in* REINVENTING DATA PROTECTION? 68 (Serge Gutwirth et al. eds., 2009). 或謂當事人同意為個人資料保護立法之核心，參見 Roger Brownsword, *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality, in* REINVENTING DATA PROTECTION? 83-109 (Serge Gutwirth et al. eds., 2009).

[318] 有學者認為應優先取得當事人同意，參見邱文聰，〈從資訊自決與資訊隱私的概念區分析「電腦處理個人資料保護法修正草案」的結構性問題〉，《月旦法學雜誌》，168 期，頁 182-184（2009 年 5 月）；劉靜怡，〈不算進步的立法：「個人資料保護法」初步評析〉，《月旦法學雜誌》，183 期，頁 153（2010 年 8 月）。有學者以為，在未經當事人同意下，以研究目的交換醫療資料，將有違必要性原則，參見 Stefaan Callens, *The Privacy Directive and Use of Medical Data for*

蓄意迴避取得「當事人同意」。本文認為仍有待斟酌。建議參考「歐盟個資指令」與英國資料保護法，將「當事人同意」置於「例外情形」之第一優先順位。[319]

此外，本項之「當事人同意」與醫界之「知情同意」概念上並不完全相同。後者多限於醫師對病人進行醫療行為前，或研究人員對參與者（資料主體）採集檢體或蒐集資料前，應獲得病人或參與者之「知情同意」(informed consent)，其規範內容較「個資法」所稱之「當事人同意」較嚴格，通常包含：能力(compentence)、揭露(disclosure)、理解(understanding)、自願(voluntariness)及同意(consent) 五項要素，亦即**具有完全能力之人，在充分瞭解研究者所揭露之重要資訊（例如）資料蒐集之程序、研究之性質與目的、資料之用途等）的前提下，本於自由意願所為同意參與研究之表示**。[320]本文認為，此概念已包含「個資法」所稱之「當事人同意」且擴及資料管理人之「告知義務」，要求資料管理人履行「知情同意」，對當

Research Purposes, 2 EURO. J. HEALTH L. 325 (1995).

「歐盟個資指令」對此則持開放態度，參見 PETER CAREY, DATA PROTECTION: A PRACTICAL GUIDE TO UK AND EU LAW 98(2004); Rouillé-Mirza & Wright, *supra* note 133, at 156. 但歐洲人權法院在 M.S v. Sweden 案([1997] 28 EHRR 313, para 34-35)有不同見解，認為「除非有歐洲人權公約第八條第二項的情形，處理個人資料仍必須取得個人同意」。換言之，非基於「國家安全、公共安全」等重大公益的情形下的個資處理，須取得資料主體同意。參見 Deryck Beyleveld & Andrew Grubb et al., *The UK Implementation of Directive 95/46/EC, in* IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE IN RELATION TO MEDICAL RESEARCH IN EUROPE 417 (Deryck Beyleveld et al. eds., 2004). European Convention on Human Rights Art 8.2(「公共機關不得干預上述權利的行使，但是依照法律的干預以及在民主社會中為了國家安全，公共安全或國家的經濟福利的利益，為了防止混亂或犯罪、為了保護健康或道德、或為了保護他人的權利與自由，有必要進行干預者，不在此限」）。

[319] Rouillé-Mirza & Wright, *supra* note 133, at 156.

[320] 參見湯德宗，〈知情同意與基因資料庫〉，《四分溪論學集：慶祝李遠哲先生七十壽辰》，頁 1009-1012（2006 年）。醫師進行「告知後同意」也為醫師的說明義務，參見楊秀儀，〈告知後同意之倫理法律再思考：縮小理論與實務的落差〉，《月旦法學》，162 期，頁 5 註 1（2008 年 11 月）。

事人之保護將較單純取得「當事人同意」更為充分，未來修法不妨參照「知情同意」之內涵，以強化敏感性個資之「當事人同意」概念，故建議新增為：「**經當事人書面知情同意**」者，得蒐集、處理或利用敏感性個資。

我「個資法」雖未將「當事人同意」列為得蒐集、處理或利用敏感性個資之豁免情形，但在其他法規中，仍有「要求資料控制人應獲得當事人同意」之規定，例如：

1. 保險法第 177-1 條第 1 項：保險或相關業者，經本人書面同意後，得蒐集、處理或利用其醫療相關資料。[321]
2. 藥品優良臨床試驗準則第 22 條第 14 款：受試者經簽署同意書，即同意相關單位得檢閱其醫療記錄。[322]

此時，公務機關或非公務機關應適用「個資法」第 6 條第 1 項但書第 1 款之「法律明文規定」，以蒐集、處理及利用該敏感性個資。

---

[321] 參見保險法(100/11/30)第 177-1 條第 1 項：「符合下列各款規定之一者，於**經本人書面同意**，得蒐集、處理或利用**病歷**、**醫療**、**健康檢查**之個人資料：一、依本法經營或執行業務之保險業、保險代理人、經紀人、公證人。二、協助保險契約義務之確定或履行而受保險業委託之法人。三、辦理爭議處理、車禍受害人補償業務而經主管機關許可設立之保險事務財團法人；第 2 項：前項書面同意方式、第一款業務範圍及其他應遵行事項，由主管機關訂定辦法管理之；第 3 項：「保險業為執行核保或理賠作業需要，處理、利用依法所蒐集保險契約受益人之姓名、出生年月日、國民身分證統一編號及聯絡方式，得免為個人資料保護法第九條第一項之告知。第 4 項：中華民國一百年六月十四日修正之本條文施行前，第一項各款之人已依法蒐集之病歷、醫療、健康檢查之個人資料，於修正施行後，得繼續處理及為符合蒐集之特定目的必要範圍內利用」。

[322] 藥品優良臨床試驗準則(99/07/19)第 22 條第 14 款：「十四、經由簽署受試者同意書，受試者即**同意其原始醫療紀錄**可直接受監測者、稽核者、人體試驗委員會及主管機關**檢閱**，以確保臨床試驗過程與數據符合相關法律及法規要求，並承諾絕不違反受試者身分之機密性」。

（二）「為履行僱傭關係之義務與權利」者

本項例外係指資料控制人(data controller)為履行「僱傭關係」(employment relationship)中之法定義務與權利，得以豁免前述限制，而例外蒐集、處理或利用敏感性個資之情形，例如法律規定公司須遵守反歧視政策，而對身心障礙員工進行健康檢查登記。[323]我「個資法」並未規定本類豁免，遇有類似情形時，應如何適用？查德國聯邦資料保護法同樣未規定本類豁免，而係直接援用「法律明文規定」豁免限制，[324]故我公務機關或非公務機關，如基於與本人間之僱傭關係，而擬蒐集、處理或利用本人之敏感性個資時，本文認為可參照德國法例，於法律明文規定雇主（公務機關或非公務機關）得蒐集、處理或利用受雇人（本人）之敏感性個資時，適用「個資法」第 6 條第 1 項但書第 1 款「法律明文規定」而豁免限制；如法律並未明文賦予雇主（公務機關或非公務機關）得以蒐集、處理或利用受雇人（本人）之敏感性個資時，則適用「個資法」第 6 條第 1 項第 2 款之「公務機關執行法定職務或私人機構履行法定義務」而豁免限制，例如依「勞工安全衛生法」第 12 條之規定，[325]雇主應要求受雇人（本人）進行健康檢查，並根據「個資法」第 6 條第 1 項但書第 2 款以蒐集、處理或利用受雇人（本人）之敏感性個

---

[323] *See* KUNER, *supra* note 34, at 2.95; BAINBRIDGE, *supra* note 132, at 56.
事實上，本款豁免存在相當大的爭議。蓋資料控制人雖得適用本款規定以處理受雇人之敏感性個資，惟基於勞雇關係之基礎，多數受雇人害怕失去工作，幾乎都會同意提供資料予資料控制人者，故此時似應適用「當事人同意」之豁免禁止要件，參見 *See* 2 ALRC, *supra* note 281, at 40.95 & 40.100.

[324] Comparative Study of European Commission Directorate-General Justice, Freedom And Security on Different Approaches to New Privacy Challenges, In Particular in the Light of Technological Developments- A.4 –Germany, at 26 (May. 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A4_germany.pdf

[325] 參照勞工安全衛生法(91/06/12)第 12 條第 1 項與第 4 項。

資。[326]

（三）「有關非營利組織之合法活動」者

有關「非營利組織之合法活動」係指：以政治、哲學、宗教或工會目的成立之基金會、協會或其他非營利團體，於其合法活動期間內，就**其會員或經常聯繫者**所為之資料處理，且其處理係經當事人同意而可以向第三人揭露者。[327]我國雖未將「工會會員資格」視為敏感性個資，惟「商業團體法」與「工業團體法」規定該團體應建立會員資料，[328]如資料內容涉及敏感性個資，例如會員之健康資料、犯罪前科等，仍應受「個資法」之拘束，適用第 6 條第 1 項但書第 2 款「公務機

[326] 我國雇主如以受雇人（本人）之健康狀況作為任用之前提條件，於健康檢查後拒絕任用受雇人，此行為雖無違反「個資法」之規定，卻有牴觸「就業服務法」之虞。按就業服務法(101/01/30)第 5 條規定，雇主對求職人或所僱用員工，不得以種族、階級、語言、思想、宗教、黨派、籍貫、出生地、性別、性傾向、年齡、婚姻、容貌、五官、身心障礙或以往工會會員身分為由，予以歧視；**其他法律有明文規定者，從其規定**。惟上開「歧視事由」示例並未包含健康資料，似**同意雇主得因雇用員工之健康狀況不明，而拒絕任用之**。*See* 2 ALRC, *supra* note 281, at 40.162.

[327] Directive 95/46/EC Art. 8(2)(d). 德國僅將此豁免項目限定於私人機構，公務機關並無此類豁免規定，參見德國聯邦資料保護法 §28(9)。奧地利、比利時、荷蘭、瑞典、英國與愛爾蘭的規定皆與「歐盟個資指令」一致。奧地利的個人資料保護準則認為，私人機構欲處理個資時，應先與「工會」(Worker Council)諮商。瑞典的報告認為「並無完整的規範以保護工作生涯中的個人完整性」，建議另訂定特別法。盧森堡的豁免相當廣泛，它允許以完成「任何特定義務或資料控制人之權利」為由，而進行處理，但仍須先取得主管機關授權。丹麥與芬蘭授權雇主與資料控制人得處理工會會員資料，因為其他相關的法律沒有類似的規定。比利時、希臘與芬蘭則嚴格規範雇主處理資料，甚至在取得當事人同意下，仍禁止處理某些資料，例如基因資訊。比利時將工會會員資格要件擴及「合作性社團」。更重要的是，法國個人資料主管機關認為，資料控制人僅得於該社團設立目的內，處理敏感性個資。因此，政治性社團無法處理會員的宗教資料，宗教性組織也無法處理會員的政治意見，參見 Korff, *supra* note 31, at 88-89.

[328] 商業團體法(98/05/27)第 5 條:「商業團體之任務如左:...七、關於會員與會員代表基本資 料之建立及動態之調查、登記事項」。工業團體法(98/05/27)第 4 條:「工業團體之任務如左:... 八、關於會員與會員代表基本資料之建立及動態調查、登記事項」。

關執行法定職務或非公務機關履行法定義務所必要者」，以蒐集、處理或利用敏感性個資。

（四）「行使法律上權利所必要」者

所謂「行使法律上權利所必須」係指資料控制人（不限於本人）為成立、行使或防禦其法律上之主張所必要者，[329]以便在法律程序中發現事實。[330]例如受雇人向雇主請求損害賠償時的就醫資料。[331]英國資料保護法規定，資料控制人於「進行法律訴訟或與其相關之活動」，或「以獲得法律建議之目的」，或「成立、行使或防禦法律之主張」所必要者，得處理敏感性個資。[332]英國資料保護署(The Information Commissioner's Office, ICO)建議本款應盡量避免適用，以能優先採用其他豁免事由為主，以防過度擴張「豁免禁止」之規定。[333]英國之保險業者係根據此項規定，處理被保險人之敏感性個資，我保險或相關業者亦根據保險法第 177-1 條，經本人書面同意後，直接適用「個資法」第 6 條第 1 項但書第 1 款「法律明文規定」，而蒐集、處理或利用其醫療相關資料。至於保險業者以外之公務機關或非公務機關，如基於行使法律上權利而須蒐集、處理或利用敏感性個資，仍須視是否有「法律明文規定」（得蒐集、處理或利用）或有法定職務或義務，否則亦不得蒐集、處理或利用敏感性個資。

---

329 Directive 95/46/EC Art. 8(2)(e); 英國資料保護法 Sche.3 6. 其他國家，例如盧森堡規定基於民事賠償所為之處理，必須基於「必要」且「唯一」之目的，並與民事訴訟程序一致，參見 Korff, *supra* note 31, at 91.

330 *See* BAINBRIDGE, *supra* note 132, at 56.

331 *See id*.

332 英國資料保護法附表三第 6 點。

333 UK Information Commissioner, *supra* note 44, para. 3.1.3.

（五）「基於醫療服務或醫學診斷」者

我「個資法」第 6 條第 1 項第 4 款規定之「公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究」豁免，有益特定機關、機構進行統計或學術研究，惟我國醫療機構基於「醫療行為」或「醫學診斷」，而須蒐集、處理或利用敏感性個資時，應如何適用？

查各國立法例普遍訂有「醫療豁免」之例外情形。[334]「歐盟個資指令」第 8 條第 3 項規定，基於**預防性醫療**(preventive medicine)、**醫學診斷**(medical diagnosis)與**照護**(care)、**治療**(treatment)**或醫療服務管理**(management of health-care services)所要求，且由**醫療事業**依國家法律或國家主管機關訂定之規則，而對職業秘密附有法定保密義務之醫療工作者，[335]或由**第三人遵守同等保密義務**者，得處理敏感性個資。[336]值得注意者，「健康照護」(health care)[337]之定義並不明確，北歐多數國家將「健康照護」視為公務機關社會服務之一部分，該公務機關可擴大「照護照顧」之範圍，甚至包含代替受照雇人所作之的財務決定(financial decision-making)。[338]本文以為，為避免公務機關或非公務機關濫用本款規定，本

[334] 英國資料保護法 Sche.3 8; 德國聯邦資料保護法 § 13(7); 澳洲隱私法「國家隱私原則」10.2 & 10.3. 比利時個資法特別就「醫療資訊」有詳細規範，參見 Consolidated text of the Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the law of December 11, 1998 implementing Directive 95/46/EC Art.8

[335] Directive 95/46/EC Recital 33

[336] Directive 95/46/EC Art.8.3

[337] 雖然美國並未立法規範敏感性個資，惟其司法判決中仍可見受到歐陸個資法的影響，例如 Nat'l Sec. News Serv. v. U.S. Dep't of Navy, 584 F. Supp. 2d 94, 96 (D.D.C. 2008)，法院認為「有關個人於醫療院所受醫療照護之記錄」係特別敏感；英國認為所謂健康照顧僅須與其「相關」，無須以「照護目的」為必要，故其範圍更加擴大，參見 *See* JOHN MACDONALD QC & CLIVE H. JONES (EDS.), THE LAW OF FREEDOM OF INFORMATION 11.18 (2003).

[338] *See* Lasse A. Lehtonen, *Genetic Information and the Data Protection Directive of the European*

款適用主體應限縮於「健康照顧機構」，且該機構須與病人有直接關連。[339]

綜上，為使醫療機構或健康照護機構，於醫療行為或醫學診斷得蒐集、處理或利用敏感性個資，我「個資法」應參考「歐盟個資指令」，**增設「醫療豁免」事項，規定「醫療機構基於醫療、診斷、或健康照護之目的」得蒐集、處理或利用敏感性個資**。否則醫療機構（包含各式護理機構、復健機構）[340]僅得適用第 6 條第 1 項但書第一款（法律明文規定）[341]或第二款（公務機關執行法定職務或非公務機關執行法定義務）[342]以蒐集、處理或利用敏感性個資，法律無規定時，醫療機構將不得蒐集、處理或利用敏感性個資。

（六）「基於重大公共利益」者

本款規定之目的在於創設一概括條款。我「個資法」並未規定公務機關或非公務機關因「重大公共利益」得蒐集、處理或利用敏感性個資。「歐盟個資指令」第 8 條第 4 項規定：**因重大公共利益，且有適當保護維護措施下，資料控制人得處理敏感性個資**。[343]所謂「公共利益」(public interest)指因「國家安全」(national security)、「社會安全」(social security)、「**刑事資料**」(criminal data)、「危機處理」(crisis management)、「人道措施」(humanitarian measures)、「退休金管理」(pension management)、「財產損害」(damage to property)等所引起的爭議。[344]英國法院認為，

Union, *in* THE DATA PROTECTION DIRECTIVE AND MEDICAL RESEARCH ACROSS EUROPE 109 (Deryck Beyleveld et al. eds., 2004).

[339] *See id.* 相同見解也獲「澳洲法改會」採用為修正建議，參見 1 ALRC, *supra* note 32, Recommendation 63-1.

[340] 參見醫療法第 31 條。

[341] 例如本文，頁 71 以下。

[342] 例如護理人員法第 24 條、助產人員法第 25 條，參見本文，頁 77 以下。

[343] Directive 95/46/EC, Art.8.4

[344] *See* David Townend, *Overriding Data Subjects' Rights in the Public Interest*, *in* THE DATA

媒體以「全版專題」報導殺人犯於「犯罪前受有之醫療措施」與「生理狀況」，合乎重大公益，並不違反資料保護法之規定。[345]此外，會員國除得因重大公共利益豁免處理敏感性個資，「歐盟個資指令」尚規定處理該敏感性個資時，須提供「適當保護措施」(suitable safeguards)，[346]該「適當保護措施」必須是指明確的(specified)且適當的(suitable)。[347]值得注意者，「科學研究」與「政府統計」，屬於因「公共利益」而豁免處理敏感性個資之情況，[348]此點與我「個資法」第 6 條第 1 項但書第 4 款（公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序）規定相同。

「歐盟個資指令」規定三種得因「公共利益」而得處理特定資料之情形。[349]第一，依「歐盟個資指令」第 8 條第 4 項，認為基於「重大公共利益」(substantial public interest)得**處理敏感性個資**；[350]第二，依「歐盟個資指令」第 3 條第 2 項規定，個

PROTECTION DIRECTIVE AND MEDICAL RESEARCH ACROSS EUROPE 97 (Deryck Beyleveld et al. eds., 2004). 法國規定須限於「保護他人生命之必要」，反之，愛爾蘭則擴大指令豁免，認為「為避免財物損失」得予以豁免處理，且該情形並不限於「資料主體依法或事實上無法給予同意」之情形，尚包括「資料處理者客觀上合理認為無法取得同意」之情形，參見 Korff, *supra* note 31, at 90-93.

345 Stone v. South East Coast Strategic Health Authority [2006] EWHC 1668 (Admin) [2007] (Eng.)

346 「歐盟個資指令」序言第 34 點：「基於重大公共利益，各國有權減損(derogation)處理敏感性個資的規定…但各國也有義務制定明確、適當的保護措施以保障個人的權利與基本隱私」。

347 事實上，「歐盟個資指令」裡存在數種有關「安全維護措施」的用語，包括 appropriate, adequate, adequate legal, suitable, suitable specific 等。此外，根據各會員國內國法的定義，「保護措施」通常指「將個人資訊編碼化、匿名化或針對個人資料使用採取保全措施」參見 Rouillé-Mirza & Wright, *supra* note 133, at 174. 各會員國以法律或授權主管機關放款豁免禁止之限制必須通知執委會，例如丹麥(§ 7(7))，參見 Rouillé-Mirza & Wright, *supra* note 133, at 158.

348 *See* Beyleveld, s*upra* note 25, at 11.

349 *See* Rouillé-Mirza & Wright, *supra* note 133, at 156-172.

350 基於重大公益，政黨於選舉過程中，得提供適當安全措施，以蒐集個人政治觀點，參見 Directive 95/46/EC Recital 36

人資料與「公共安全」(public security)、「國防」(defence)、「國家安全」(state security)或「刑法有關之活動」(activities relating to criminal law)相關者，**完全不適用「歐盟個資指令」規範**；第三，依「歐盟個資指令」第 13 條規定，各會員國得基於國家安全(national security)、國防(defence)、公共安全(public security)等理由，限制包括當事人之「受告知權」與「接觸權」等，亦即**部分排除適用「歐盟個資指令」**。一般認為，**前開三種情況皆可作為依據而處理敏感性個資**，例如適用第 8 條第 4 項（豁免禁止處理敏感性個資之規定）或適用第 3 條第 2 項（排除適用「歐盟個資指令」所有規範）。[351]

我「個資法」未規定「基於重大公共利益」得蒐集、處理或利用敏感性個資，為避免妨礙國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益公共安全，本文建議應參考「歐盟個資指令」，**增訂**（公務機關或非公務機關）概括條款—**「為保護重大公共利益所必要」得蒐集、處理或利用敏感性個資**。

（七）「為維護當事人重大利益」者

我「個資法」未規定公務機關或非公務機關「為維護當事人（本人）之重大利益」得例外蒐集、處理或利用敏感性個資。「歐盟個資指令」第 8 條第 2 項c款規定，**當事人（本人）實質或依法不能表示同意**時，為**保護當事人（本人）或第三人重大利益**(vital interest)**必要**，得豁免處理敏感性個資；[352]德國聯邦資料保護法第 13 條第 2 項第 3 款規定，為保護資料主體或第三人之重大利益(vital interest)，

[351] *See id.*

[352] Directive 95/46/EC, Art.8.2 (c) "processing is necessary to protect the *vital interests* of the data subject or of another person where the data subject is *physically* or *legally incapable* of giving his consent." (emphasis added).

而資料主體基於生理或法律上原因而無法表示同意時，得蒐集敏感性個資；[353]澳洲隱私法規定，為避免或預防對任何人之重大且急迫之威脅，於資料主體生理上或法律上無行為能力，或能力無法表達同意時，得蒐集敏感性個資。[354]無法表示同意之資料主體可能包括「孩童」或「智能有缺陷」的人，[355]或是受到嚴重意外而失去意識之人。[356]

此處的「重大利益」(vital interest)與前述所稱「實質公共利益」(substantial public interest)有所不同，「歐盟個資指令」序言第 31 點揭示，為了保護資料主體之重要生存利益，所進行之個人資料處理，須被視為是合法。因此，所謂「重大利益」應視為「保護生命之所必要」[357]或「保護資料主體生存之重要利益」，[358]例如於交通事故發生後，揭露當事人之醫療紀錄給醫療機構。[359]「歐盟個資指令修正案」認為，保護第三人之重大利益時，須「資料主體實質或依法不能同意表示」，惟此一要件將妨礙拯救他人生命。蓋當事人非依法不能同意，而係主動拒絕同意時，將無法適用本款規定以保護他人生命，爰建議刪除之。[360]綜上，為保護本人之生存重要利益，我「個資法」應參照前揭各國法例，增訂「**為保護當事人之重大利益所必要」得蒐集、處理或利用敏感性個資**。

---

[353] 德國聯邦資料保護法 §13(2)3.

[354] 澳洲隱私法「國家隱私原則」10.1(c).

[355] *See* Nys, *supra* note 308, at 53.

[356] 前提必須是資料主體「能」提供同意，而非「不能」。參見 BAINBRIDGE, *supra* note 132, at 56.

[357] 英國資料保護法(Sch.2 4)，本款限適用於「本人以外之第三人」，此點與「歐盟個資指令」規範不同。

[358] Directive 95/46/EC Recital 31.

[359] UK Information Commissioner, *supra* note 44, para. 3.1.1

[360] *See* Data Protection Directive (95/46/EC) Proposals for Amendment made by Austria, Finland, Sweden and the United Kingdom, Explanatory Note, *supra* note 105, Proposal (2)9.

第三節 小結

鑑於敏感性個資之特質，其蒐集、處理或利用將嚴重侵害個人隱私，故各國立法例與我「個資法」原則皆禁止蒐集、處理或利用敏感性個資，僅於例外情形得蒐集、處理或利用敏感性個資。我「個資法」規定四種例外得蒐集、處理或利用敏感性個資之情形，惟其意義猶有澄清之必要，析言之：

一、「個資法」規定四種例外情形，定義應予釐清

1. 所謂「法律明文規定」應限「法律明定公務機關或非公務機關，得蒐集、處理或利用敏感性個資」者。「法律」應指「立法院三讀通過，總統公布施行之法律」。此為「個資法」須「優先適用其他法律」之情形，限於「其他法律有特別規定（個資之蒐集、處理或利用）者」（無論寬嚴）， 其他法律無特別規定（個資之蒐集、處理或利用）時，仍一律適用「個資法」。

2. 所謂「公務機關執行法定職務或私人機構履行法定義務」應限於「公務機關或非公務機關基於其法定職務或義務所必要，須蒐集、處理或利用者」。同時，該蒐集、處理或利用行為須合乎「必要」且須提供「適當安全維護措施」。「必要」須考量其處理之目的是否合法、處理該個人資料是否為唯一達成該目的之手段、其處理與追求之目的不得顯失均衡；「適當安全措施」須注意防止個人資料被竊取、竄改、毀損、滅失或洩漏，並採取技術上及組織上之必要措施。

3. 所謂「當事人自行公開」係指當事人自行對不特定人或特定多數人為揭露；所謂「其他已合法公開」則指依法規公示、公告或以其他合法方式公開之

個人資料，此「合法公開」之行為應視為個人資料之「利用」，須遵守「個資法」相關規定。

4. 所謂「公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序」，其目的須限於「醫療、衛生或犯罪預防」與「統計或學術研究而有必要」，本文建議將「統計或學術研究」用語改為「科學研究」代替；有關「學術研究機構」之定義不明，為合理促進學術研究發展，建議擴大定義為包括國立研究院及公私立大學研究所或其他公私立研究機構；有關「一定程序」之定義同樣不明，為求「個資法」用語統一且確保本款適用之個人資料無法識別特定當事人，本文建議以「經過匿名化處理，或依其揭露方式無從再識別特定本人」，代替「一定程序」之用語。

二、建議新增四類例外得蒐集、處理或利用敏感性個資之情形

我「個資法」僅訂有四種例外得蒐集、處理或利用敏感性個資之情形，相較各國立法例多達八至十類，顯有不足。茲建議，參照各國立法例，增訂四類例外情形，包括「經當事人書面同意」、「基於預防性醫療、醫學診斷、健康照護之目的」、「為保護重大公共利益所必須」與「為保護當事人之重大利益」時，得蒐集、處理或利用敏感性個資，試修正「個資法」第 6 條第 1 項之條文為：

一、經當事人書面同意。

二、法律明文規定者。

三、公務機關執行法定職務或非公務機關履行法定義務所必要。

四、資料已經當事人自行公開或由其他已合法公開之個人資料。

五、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為科學研究而有必要，且資料須經過匿名化處理，或依其揭露方式無從再識別特定本人，但資料經匿名化處理後無法進行研究者除外。

六、醫療機構基於預防性醫療、醫學診斷、健康照護之目的

七、基於重大公共利益所必要

八、為維護當事人重大利益所必要

第四章　敏感性個人資料與個人資料保護原則

本文於清楚界定「敏感性個資之定義」（本文第二章）與研究各種「豁免禁止，例外得蒐集、處理或利用敏感性個資之情形」（本文第三章）後，本章擬討論：公務機關或非公務機關於蒐集、處理及利用敏感性個資時，所應遵循之「個人資料保護原則」。以下先簡介「個人資料保護原則」之概念，再依敏感性個資之「蒐集」、「處理」及「利用」三個操作流程，分項討論各種「個人資料保護原則」。

第一節　個人資料保護原則

「個人資料保護原則」(Personal Data Protection Principles)泛指資料控制人於蒐集、處理或利用個資時，應履行之保護義務。按OECD「個人隱私與跨境個人資料流通保護綱領」（下稱「OECD 個資綱領」）[361]規定八項「個人資料保護原則」，包括：

1. 蒐集限制原則(Collection Limitation Principle)[362]
2. 資料品質原則(Data Quality Principle)[363]
3. 目的特定原則(Purpose Specification Principle)[364]

---

[361] OECD Guidelines on the Protection of the Privacy and Transborder Flow of Personal Data, §§ 7-14 [*hereinafter* OECD Guidelines].

[362] OECD Guidelines § 7 ("There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject"). 個人資料之蒐集應予限制，且個人資料應以合法且公平(lawful and fair)之方法獲得，適當時應通知本人或獲得其同意。

[363] OECD Guidelines § 8 ("Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date"). 個人資料應與其欲使用(use)之目的相關，並限於該目的之必要範圍，且應確保資料正確(accurate)、完整(complete)與更新(up-to-date)。

4. 利用限制原則(Use Limitation Principle)[365]：

5. 安全保護原則(Security Safeguards Principle)[366]：

6. 公開原則(Openness Principle)[367]

7. 個人參與原則(Individual Participation Principle)[368]

8. 責任歸屬原則(Accountability Principle)[369]

「歐盟個資指令」以「資料品質原則」(Data Quality Principle)作為其「個人資料保護原則」。所謂「資料品質原則」規定在「歐盟個資指令」第 6 條，各會員國

---

[364] OECD Guidelines § 9 (“The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose”).

[365] OECD Guidelines § 10 (“Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
a) with the consent of the data subject; or
b) by the authority of law”).

[366] OECD Guidelines § 11 (“Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data”).

[367] OECD Guidelines § 12 (“There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller”).

[368] OECD Guidelines § 13 (“An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended”).

[369] OECD Guidelines § 14 (“A data controller should be accountable for complying with measures which give effect to the principles stated above”).

（資料控制人）應確保個人資料須：[370]

1. 公平且合法(fairly and lawfully)處理。
2. 資料之蒐集(collection)目的應特定(specified)、明確(explicit)且正當(legitimate)，資料之處理(processing)須非與原始蒐集目的顯不相容(incompatible)。
3. 蒐集、處理資料應適當(adequate)、相關(relevant)且不逾越原始目的。
4. 保持資料正確(accurate)、完整(complete)與更新(up-to-date)。
5. 以可得辨識資料主體之格式儲存資料者，其蒐集及處理不得逾越原目的之必要期間。

上開「個人資料保護原則」影響各國個人資料保護立法，[371]惟各國立法規範之方法並不相同。大體而言，有仿效上開「OECD個資綱領」與「歐盟個資指令」，特別設立「個人資料保護原則」章節之立法，例如英國資料保護法(Data Protection Act 1998)[372]與澳洲隱私法(Privacy Act 1988)。[373]有未使用「個人資料保護原則」用語且未設有專門章節，而將「個人資料保護原則」分散規定於個人資料保護法中之立法，例如德國聯邦資料保護法(Bundesdatenschutzgesetz)與日本個人資料保護法。[374]

---

[370] Directive 95/46/EC, Art.6

[371] *See* CAREY, *supra* note 318, at 51.

[372] 英國資料保護法附表一(Schedule 1)。

[373] 澳洲隱私法第三段第二部份(Part III Division 2)之「資訊隱私原則」(Information Privacy Principles)與附表三之「國家隱私原則」(National Privacy Principles)，前者適用於公部門，後者適用於私人機構。

[374] 個人情報の保護に関する法律，平成 15 年 5 月 30 日法律第 57 号。

我「個資法」受德國影響，亦未使用「個人資料保護原則」用語，也未設專章規定「個人資料保護原則」，有關公務機關或非公務機關應履行之保護義務，散見於「個資法」各規定中。本文認為，「個人資料保護原則」概念廣泛，如能清楚定義、宣示「個人資料保護原則」，有助於任何人理解資料控制人之保護義務；且資料控制人將易於自行檢視其進行之資料「蒐集、處理或利用」行為，是否確實履行個人資料之保護義務。本文以下將依「OECD 個資綱領」之八項「個人資料保護原則」作為主要架構，並參考「歐盟個資指令」之規定，增加「期間限制原則」與「國際傳輸」兩項原則，形成十項「個人資料保護原則」（如圖一）並依敏感性個資之「蒐集」、「處理」、「利用」，分項檢視公務機關或非公務機關應遵循之保護義務。

圖一：蒐集、處理或利用敏感性個資時，公務機關或非公務機關適用個人資料保護原則之情形

第二節　敏感性個資之「蒐集」相關原則

按「個資法」第 2 條第 3 款，「蒐集」係**指以任何方式「取得」個人資料**。[375] 資料蒐集之方式可分為「直接蒐集」(directly from an individual)或「間接蒐集」(from someone other than the individual)。「直接蒐集」，係指資料控制人直接向本人（當事人）取得個人資料；[376]「間接蒐集」，係指資料控制人非向本人（當事人）直接蒐集資料，而向第三人取得個人資料。[377]資料之蒐集發生於資訊循環流動(cycle)的最初階段。資料未經「蒐集」，將不會產生「處理」或「利用」等其他問題。[378] 以下分項討論公務機關或非公務機關「蒐集」敏感性個資時，應適用之各種個人資料保護原則。

一、蒐集限制原則

「蒐集限制原則」(Collection Limitation Principle)係指：個人資料之**蒐集應予限制**，且個人資料應以**合法且公平**(lawful and fair)之方法獲得，適當時須通知本人

---

[375] 德國聯邦資料保護法(§ 3(3))定義：「蒐集」係指「獲得」(acquisition)個人資料；澳洲「法律改革委員會」(Australian Law Reform Commission)認為：「蒐集」為「接收」(receipt)與「保留不請自來」(retention of unsolicited)之個人資訊。所謂「不請自來」之資訊係指公務機關或私人機構，未採取任何主動措施而獲得之資訊，此類資訊隨著科技發展相形增加，例如社區機構收到家庭暴力相關資訊，相關討論參見 1 ALRC, *supra* note 32, at 720-726.

[376] 參見「個資法」第 8 條第 1 項規定：「公務機關或非公務機關…向當事人蒐集個人資料時，應明確告知…」。

[377] 參見「個資法」第 9 條第 1 項規定：「公務機關或非公務機關…蒐集非由當事人提供之個人資料…」。

相較於我「個資法」將「間接蒐集」定義「非由當事人提供」，各國立法例略有不同。德國聯邦資料保護法(§ 4(2))定義為「資料主體未參與之蒐集」；英國資料保護法則未規定「間接蒐集」。至於**本人（當事人）是否知情，僅影響資料控制人是否得以據此豁免告知義務而已**。

[378] *See* 1 ALRC, *supra* note 32, at 21.1.

並獲得其同意。[379]此為個人資料保護之主要原則，並據此衍生出其他原則。[380]所謂「合法」之方法，係指**資料控制人須依法蒐集個人資料**；[381]「公平」之方法，則與「通知本人」相關，係指資料控制人將如何使用蒐集而來之個人資料，向本人透明化(transparent)，[382]亦即資料控制人須向本人履行「告知義務」。[383]以下將本原則分為「合法蒐集原則」與「告知義務」，分別討論。

（一）合法蒐集原則

按「個資法」第 5 條規定：「個人資料之**蒐集**、處理或利用，**應尊重當事人之權益，依誠實及信用方法為之…**」，此為個人資料之合法蒐集原則；第 6 條第 1 項規定：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限…」，此為敏感性個資之「合法蒐集原則」。原則上，公務機關或非公務機關禁止蒐集敏感性個資；於符合本項但書例外規定情形時，得例外蒐集敏感性個資，故公務機關或非公務機關蒐集敏感性個資，除需尊重本人權益，以誠信方法外，尚須符合第 6 條第 1 項但書各款事由之

---

379 OECD Guidelines § 7 (“There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject”).

380 *See* Bygrave, *supra* note 120, at 3.2

381 合法之意涵，或可藉由理解「非法」之概念予以釐清，所謂非法為某行為「與法律、法規規定相左，或未具備合法正當性與抗辯之事由」參見 UK Information Commissioner, *supra* note 44, para. 3.1.4

此外，資料控制人雖符合「合法蒐集原則」，但非謂資料控制人即不受控制。申言之，即便資料控制人得基於公益、法律明文規定或其他合法權益，處理該個人資料，但**本人（當事人）仍有權利，反對資料控制人進行任何資料處理**，參見本節後述與 Directive 95/46/EC Recital 45 & Art.14

382 *See* UK ICO, The Guide to Data Protection, at 44, *available at* http://www.ico.gov.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/THE_GUIDE_TO_DATA_PROTECTION.ashx

383 *See* MACDONALD QC & JONES (EDS.), *supra* note 337, at 8.2.1.1; 1 ALRC, *supra* note 32, at 23.121.

一。有關本條但書各款情形，已如第三章所述，不贅。

（二）告知義務

按「個資法」第 8 條第 1 項規定：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項…」；第 9 條第 1 項規定：「公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項…」。此為公務機關與非公務機關之「告知義務」。

猶須注意者，依上開規定，公務機關或非公務機關須「依個資法第 15 條或第 19 條」蒐集個人資料，才需要履行告知義務。惟「個資法」第 15 條規定：「公務機關對個人資料之蒐集或處理，**除第六條第一項所規定資料外**，應有特定目的，並符合下列情形之一者…」;第 16 條規定:「非公務機關對個人資料之蒐集或處理，**除第六條第一項所規定資料外**，應有特定目的，並符合下列情形之一者…」，第 6 條第 1 項所規定者為敏感性個資，「個資法」第 15 條與第 19 條排除敏感性個資，將使公務機關或非公務機關蒐集或處理敏感性個資時，無須履行告知義務。有關第 15 條與 19 條「除第六條第一項所規定資料外」之用語，經查為「個資法」修正時所新增，立法說明謂：此用意僅在於使公務機關或非公務機關逕依第 6 條第 1 項但書之規定，以蒐集、處理敏感性個資，而無須適用第 15 條或第 19 條蒐集、處理敏感性個資；[384]且查遍英、德、澳洲等國立法例，皆無類似規定，資料控制人蒐集、處理或利用敏感性個資時，仍須履行告知義務。故本文認為，此應為明

[384] 依 2009 年 11 月 12 日「立法院朝野黨團協商結論」，於「個資法」第 15 條與第 19 條新增「除第六條第一項所規定資料外」之用語，其修正說明謂：「本條僅適用於一般個人資料，特種資料之蒐集或處理，仍應依本法第六條規定為之」，參見立法院公報，99 卷 29 期，頁 376。

顯立法疏漏，**應將第 8 條或第 9 條條文前段所謂「依第十五條或第十九條規定」用語改為「依本法規定」，始能將敏感性個資納入本條規範內，以要求公務機關或非公務機關履行告知義務**。

要求資料控制人履行告知義務，將 1. 使本人得以知悉資料控制人擁有其個人資料之事實，並得以行使「個資法」所賦予之權利，蓋當事人不知其資料即將為資料控制人所蒐集，焉能行使其個人權利；[385]2. 有助於資料控制人確保資料之正確(accurate)、完整(complete)與適時更新(up-to-date)，亦即履行「資料品質原則」（後詳）。[386]告知方式得以書面、電話、傳真、電子文件或其他適當方式。[387]「個資法」第 8 條與第 9 條，將公務機關或非公務機關之告知義務，依資料蒐集之方式分為「直接蒐集之告知義務」或「間接蒐集之告知義務」，以下分點述之。

1. 「直接蒐集」之告知義務

「個資法」第 8 條第 1 項規定，公務機關或非公務機關依第 15 條或第 19 條規定，向當事人「直接」蒐集個人資料，應於「向當事人**蒐集時**」，[388]告知下列事項：「公務機關或非公務機關名稱；**蒐集之目的**；個人資料之類別；個人資料利用

---

385 *See* Rouillé-Mirza & Wright, *supra* note 133, at 163.

386 *See* 1 ALRC, *supra* note 32, at 23.121 英國規定資料控制人應向主管機關 ICO 登記註冊，始得處理個人資料，參見英國資料保護法 §17。

387 參照「個資法施行細則草案」第 13 條；呂丁旺，〈淺析修正「個人資料保護法」〉，《月旦法學》，183 期，頁 136（2010 年 8 月）。近日行政院宣布將修改「個資法」，未來告知之形式將不限於紙本，電子文件亦可，參見聯合新聞網，〈個資法啟動修訂 將擴大保護對象〉，2012 年 2 月 17 日，網址：http://udn.com/NEWS/NATIONAL/NAT4/6904976.shtml 最後瀏覽日期：2012/03/06。

388 「歐盟個資指令」並未就此時點予以規範，相較之下我「個資法」更顯進步！

之期間、地區、對象及方式；當事人依第三條規定得行使之權利及方式；當事人得自由選擇提供個人資料時，不提供將對其權益之影響」。公務機關或非公務機關**直接**向本人蒐集敏感性個資，除須告知前項內容外，尚須告知**本人其**（公務機關或非公務機關）**據以蒐集之「豁免禁止」條款**（第 6 條第 1 項但書），且該條款**須符合其蒐集之目的**。

至於豁免告知本人之情形，依「個資法」第 8 條第 2 項規定，具有下列五款情形之一者，公務機關或非公務機關**免於告知本人**（當事人）:「一、**依法律規定得免告知**。二、**個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要**。三、告知將妨害公務機關執行法定職務。四、告知將妨害第三人之重大利益；當事人明知應告知之內容[389]」。上開五項「豁免告知」事由中，第二款「個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要」，其要件與「個資法」第 6 條第 1 項但書第 2 款幾乎相同。[390]因此將**使公務機關或非公務機關依「個資法」第 6 條第 1 項但書第 2 款**（公務機關執行法定職務或非公務機關履行法定意義所必要，且有適當安全措施）**蒐集敏感性個資時，可適用第 8 條第 2 項規定，而免於履行告知義務**，此「豁免告知」之範圍，是否過當，仍須斟酌。查「歐盟個資指令」僅規定一種豁免告知事由:「資料主體已經知悉者」[391]；德國「聯邦資料保護法」規定，於下列情形之一時，豁免告知本人：本人已透過其他方式知悉資料之儲存(storage)與傳輸(transfer)；告知本人須付出極不合理(disproportionate)之代價；[392]法律已明定個資之保存與傳輸。上開立法例之「豁免告知」事由皆未有「公務機關或非公務機關因執行法定職務或義務而蒐集敏感性

---

389 此豁免為比較法上常見之項目，參見 Directive 95/46/EC Art. 10 &11; 德國聯邦資料保護法 §19a

390 後者多要求資料控制人應「且有適當安全維護措施」。

391 相較之下，參見 Directive 95/46/EC Art.10.

392 參見德國聯邦資料保護法 §19a

個資」之情形，為避免公務機關或非公務機關以執行職務或義務為由，於蒐集敏感性個資時豁免告知當事人，本文認為，**公務機關因執行法定職務或非公務機關因履行法定義務而蒐集敏感性個資時，應排除適用「個資法」第 8 條第 2 項第二款之「豁免告知」規定，亦即公務機關或非公務機關蒐集敏感性個資時，仍須履行告知義務，向本人告知**。

2. 「間接蒐集」之告知義務

「個資法」第 9 條第 1 項規定：「公務機關或非公務機關依第十五條或第十九條規定蒐集**非由當事人提供**之個人資料，應於**處理或利用前**，向當事人告知**個人資料來源**及**前條第一項第一款至第五款所列事項**」[393]，此為「間接蒐集」之告知義務。本條規定，公務機關或公務機關應於個資「**處理或利用前**」[394]，履行告知義務，蓋此時資料已經被第三人所蒐集（掌握），資料控制人係透過第三人所提供之資料以進行處理，故僅得於「處理或利用前」通知資料之本人。公務機關或非公務機關應告知下列事項：「**個人資料來源**；公務機關或非公務機關名稱；**蒐集之目的**；個人資料之類別；個人資料利用之期間、地區、對象及方式；當事人依第三條規定得行使之權利及方式」。公務機關或非公務機關蒐集第三人所提供之敏感性個資，除須於處理或利用前告知上開六種事項外，尚須告知**本人：其**（公務機關或非公務機關）**據以蒐集之「豁免禁止」條款**（第 6 條第 1 項但書），且該條款**須符合其蒐集之目的**。[395]

---

[393] 德國聯邦資料保護法 §§ 19(1) & 34(1)；澳洲隱私法並未規定資料管理人須告知資料來源，參見 1 ALRC, *supra* note 32, at 23.162.

[394] 「歐盟個資指令」(Art.11(1))規定於「首次儲存個人資料」或「向第三人揭露」時，應告知資料主體。

[395] 依據「目的特定原則」（後詳），資料控制人應告知當事人其處理目的，及其於特殊情況下須處理之資料，上述通知同樣須於首次處理前完成，參見 MACDONALD QC & JONES (EDS.), *supra* note

「個資法」第 9 條第 2 項規定，具有下列五款情形之一者，資料控制人免於告知當事人：有前條第二項所列各款情形之一、**當事人自行公開或其他已合法公開之個人資料**；不能向當事人或其法定代理人為告知；**基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限**；大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。[396]其中，第一款規定與前條第 2 項（第 8 條第 2 項）所規定之五種事由相同，另外加上本項四款情形，使本項規定之「豁免告知」事由將多達九種。

本項第二款「當事人自行公開」與第 6 條第 1 項但書第 3 款規定相同，公務機關或非公務機關蒐集第三人所提供之「本人自行公開之敏感性個資」，**將無須告知本人**。

本項第四款規定「基於**公共利益**為統計或學術研究之目的而有必要，且該資料須**經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限**」得免於告知本人。所謂「資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人」係指個人資料以代碼、匿名或其他揭露方式，無從辨識該特定個人，或需費過鉅或耗時過久始能予以辨識者。[397]本款規定與第 6 條第 1 項但書第 4 款規定類似，主要差別有二：1. 本款未限定適用主體，第 6 條第 1 項但書第 4 款限適用「公務機關或學術研究機構」；2. 本款之主要目的為「基於公共利益」，第 6 條第 1 項但書第 4 款限「基於醫療、衛生或犯罪預防」，公共利益概念上應包含醫療、衛生或犯罪預防。綜上所述，本款適用範圍其實較第 6 條第 1 項但書第 4 款

337, at 10.25.

396 參照「個資法」第 9 條第 2 項。

397 此為「匿名化」之概念，參照「個資法施行細則草案」第 14 條。

為廣，**公務機關或學術機構依第 6 條第 1 項但書第 4 款（間接）蒐集敏感性個資時，得適用本款，豁免告知本人**。

本項第五款規定「大眾傳播業者基於新聞報導之公益目的而蒐集個人資料」得免於告知本人。大眾傳播業者如欲蒐集敏感性個資，以進行有關傳染病擴散、性侵害犯罪之報導時，是否免於告知本人，仍有疑義。大眾傳播業者須先適用「個資法」第 6 條第 1 項但書所規定之四種情形之一，以蒐集敏感性個資。大眾傳播業者所進行者因不屬第 6 條第 1 項但書第 4 款所謂之「為統計或學術研究」，故大眾傳播業者僅得適用其餘三款規定。查我國現行法並無有關「大眾傳播業者得蒐集敏感性個資」（第 6 條第 1 項但書第 1 款）之規定，有關「大眾傳播業者執行法定職務或法定義務」（第 6 條第 1 項但書第 2 款）者，僅有中央通訊社[398]，其他**大眾傳播業者，僅能蒐集「當事人自行公開或其他已合法公開」**（第 6 條第 1 項但書第 3 款）**之敏感性個資**。該**敏感性個資若屬「直接蒐集」者，大眾傳播業者則須履行告知義務**（第 8 條第 2 項），若屬**「間接蒐集」者，大眾傳播業者始免於告知本人**（第 9 條第 2 項）。惟此一區分是否有實益，仍有待研究。大眾傳播業者為便宜行事，**有可能一律採用「間接蒐集」之方式以迴避適用「直接蒐集之告知義務」**。各國立法例對於大眾傳播業者多採開放立場，立法明定「新聞豁免」排除適用個人資料保護法。[399]本文建議，為合理權衡新聞自由與個人資料保護，有關大眾傳播業者合理蒐集、處理或利用敏感性個資以進行新聞報導之情形，可考慮放寬限制，仿照各國立法，部分或全部排除適用「個資法」之規定。

---

[398] 參見中央通訊社設置條例(88/01/20)第 3 條：「本社之任務如左：一、辦理國內外新聞報導業務，服務大眾傳播媒體。二、辦理國家對外新聞通訊業務，促進國際對我國之瞭解。三、加強與國際新聞通訊社合作，增進國際新聞交流」。

[399] 參見 Directive 95/46/EC Recital 37 & Art. 9; 德國聯邦資料保護法 §41；英國資料保護法 §32；澳洲隱私法 §7B(4)，比較法之詳細發展可參見 2 ALRC, *supra* note 281, at 1439-1471.

3. 蒐集後變更原始目的仍須告知本人

資料控制人嗣後變更目的，使蒐集之目的與利用之目的不同時，應如何處置？我「個資法」並未規定，本文認為，應參考日本「個人資料保護法」[400]規定，解為：資料控制人變更利用目的後，重新通知本人。[401]故此時應將該資料視為「未履行告知義務」，**資料控制人須重新通知本人**。

4. 新興科技發展影響資料控制人之告知義務

近年隨著科技發展，資料蒐集之方式已產生變化，許多蒐集方式已不限於「實體」之資料流動（例如紙本文件），而屬於「無形」之資料流動，且屬「直接」與「間接」向本人蒐集者，例如網路蒐集、無線射頻識別，以下分項簡述之。

(1) 網路蒐集

所謂網路蒐集，指資料控制人透過網路，以使用特定電腦配備或程式，直接或間接取得個人資料。由於此種蒐集資料之方法，無需經過本人同意，較常引起爭議。[402]通常可蒐集之資料包括：1. 使用搜尋引擎提供之免費電子郵件與地圖搜尋服務；2. 網站瀏覽紀錄；3. 本人於網路上購買之商品與服務。上開資料皆有可

[400] 個人情報の保護に関する法律，平成 15 年 5 月 30 日法律第 57 号。

[401] 日本個人資料保護法 §§ 18(3) & 23(3)，其餘參見 MORGAN & BOARDMAN, *supra* note 120, at 8.3.5.6.

[402] *See* 1 ALRC, *supra* note 32, at 9.16.

能屬於敏感性個資，[403]其方式略有以下數種：

I. Cookies

此為自特定電腦或網站發出的細微資訊，將傳遞至使用者的網路瀏覽器程式內，而（自動或非自動）儲存於使用者電腦中。當同一使用者再次造訪該同一網站時，該資訊便會傳遞回網站，藉以識別使用者之身份。[404] Cookies之目的在於建立專屬個人化的網路服務。[405]原則上，使用者可以藉由瀏覽器之設定，控制Cookies之存取權限與存續期間。[406]為保護電子通訊領域(electronic communication sector)之個人資料保護，歐盟執委會(European Commission)在 2002 年發佈「隱私與電子通信指令」(Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector)[407]，該「隱私與電子通信指令」的前言提到：因為安裝Cookies後，他人便得以接觸終端機系統(terminal equipment)與儲存於類似系統中之敏感性隱私資訊，故使用者應有權拒絕安裝Cookies（或類似裝置）於他們的終端機系統。[408]此外，「隱私與電子通信指令」並規定各會員國應確保本人知悉Cookies之蒐集目的，並提供「退出」權(opt-out)，以提供本人拒絕安裝Cookies之機會。

---

403 *See id.*

404 *See id.* at 9.18.

405 *See id.* at 9.19.

406 *See id.* at 9.20.

407 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. [*hereinafter* DPEC]

408 DPEC Ricital 25.

II. 「超文件傳輸協定」(Hypertext Transfer Protocol, HTTP)

「超文件傳輸協定」是一種能夠使資訊在網路上傳送與接收的規則(rule)。[409]使用者為了接觸網站，網路瀏覽器必須向網路傳送資訊，例如網址(Uniform Resource Locator, URL)。傳送的過程中有可能揭露使用者之電子郵件或瀏覽網頁之紀錄，更可藉由網路服務供應商(Internet Service Provider, ISP)識別使用者之個人身份。

(2) 「無線射頻識別」(Radio Frequency Identification, RFID)

「無線射頻識別」係由「轉發器」(transponder or RFID Tag)、「感應器」(reader)與「後勤辦公室」(back office)三者所構成。「轉發器」將資訊傳送至「感應器」，「感應器」再將資料傳送至「後勤辦公室」，以蒐集相關資料。[410]「轉發器」傳送之資料相當有限，多限於可識別之編號，常用於產品監測、個人追蹤、出入管制與健康照護等。[411]我國建置之國道高速公路收費系統，最新系統即採用「無線射頻識別」技術。[412]「轉發器」可植入人體，並儲存各類敏感性個資，例如醫療資訊。[413]

以上皆為資料控制人使用新興科技方式以蒐集敏感性個資之例示。依我「個資法」第 8 條與第 9 條，公務機關或非公務機關蒐集個人資料時，應履行告知義

---

[409] *See id.* at 9.23.

[410] Andreas Kruse et al., Final Report, The Regulatory Framework for RFID, at 13 (Aug. 2008), *available at* www.rfid-in-action.eu/public/results/legal-aspects/framework.pdf

[411] *See id*.

[412] 自由電子報，〈ETC 挫敗 遠通改推免費 eTag〉，2011/07/01，網址 http://www.libertytimes.com.tw/2011/new/jul/1/today-t2.htm （最後瀏覽日期 2012/02/10）。

[413] 美國食品及藥物管理局(Food and Drug Administration)已批准使用「無線射頻識別」裝置於人體，參見 Michael E. Burke et al., *Infonnation Services, Technology, and Data Protection*, 39 INT'L LAW 403, 408-409 (2005).

務，惟公務機關或非公務機關使用上開各類方式以蒐集個資時，其應使用之告知方式、應告知之事項與告知之時點，是否須配合資料之蒐集之方式而予以調整，仍有待研究。查「澳洲法改會」(Australian Law Reform Commission, ALRC)建議，資料主管機關應針對「資料控制人使用新興科技蒐集個資之事項」發佈規範準則，該準則應釋明：[414]

- 新興科技之定義，例如 RFID 與 Cookies
- 資料控制人得以新興科技蒐集個人資料之情形
- 資料控制人應履行告知義務之時點（蒐集時或蒐集前）
- 資料控制人應履行之告知事項（須包含有關新興科技之使用特徵）
- 資料控制人所蒐集之資料形式或類型

本文認為，公務機關或非公務機關使用上開方式蒐集敏感性個資時，可參考上開建議，主動增加告示事項之內容，而不限「個資法」第 8 條或第 9 條所定之事項。本文亦建議，各目的事業主管機關，可針對各目的事業內使用新興科技蒐集敏感性個資之情形，發佈解釋函予以釋明。

二、個人參與原則

個人參與原則通常指個人對於有關自身之資料 [415]，應有：[416]接觸權(right of

[414] *See* 1 ALRC, *supra* note 32, at 30.

[415] 個人資料之內容如涉及第三人者，資料控制人應符合「個資法」第 15 條或第 19 條之規定，並通知該當事人（第三人），否則不應提供予申請之本人，有關告知義務請參見本章第二節。英國資料保護法(§ 7(6))規定資料控制人應考量：本人向第三人是否負有保密義務、任何獲得第三人同意之方法、第三人是否有能力給予同意及第三人有無明確拒絕之意思表示。此外，資料控制人亦可遮掩資料內第三人姓名或其他可得辨識出他人之資料，始提供予申請之本人，參照英國資料保護法 § 7(5)。

access)[417]；更正、封鎖或刪除權(right of correction or erasure)[418]；拒絕權(right to object)；[419]賠償請求權(right to compensation)[420]；拒絕行銷權(right to prevent direct marketing)[421]與拒絕自動化決定權(right to prevent automated decision-taking)[422]。「個資法」第 3 條規定之個人權利包括：查詢或請求閱覽權、請求製給複製本權、請求補充或更正權、請求停止蒐集權、處理或利用權[423]與請求刪除權。上述權利並落實於第 10 條（答覆查詢、提供閱覽、製給複製本）與第 11 條（請求補充、更正、停止蒐集、處理或利用），該權利並不得預先拋棄或特別限制。[424]

依「個資法」第 10 條規定，本人得向公務機關或非公務機關查詢其所蒐集之

---

[416] *See* MORGAN & BOARDMAN, *supra* note 120, at 10.1.2; 例如「OECD 個資綱領」第 13 條；「APEC 隱私框架」第 23 點；英國資料保護法第 6 原則規定：個人資料之處理應符合本人（資料主體）依本法規定之權利。「歐盟個資指令」賦予當事人數種權利：(1) 自資料控制人處知悉與其相關之個人資料是否正被處理、其處理目的、對何人揭露與個人資料之來源(Art. 12(a))；(2) 知悉自動處理程序之邏輯構造(Art. 12(a))；(3) 資料處理不符合本指令規定時，資料主體有修正、刪除或封鎖處理之權(Art. 12(b))；(4) 以重大正當之理由，反對個人資料被處理之權(Art. 14(a))；(5) 反對個人資料被用於直接行銷之權(Art. 14(b))；(6) 不會基於依據自動化資料處理個人資料之結果，而使資料主體之決定受到限制(Art. 15(1))，相關討論參見 Deryck Beyleveld, *The Duty to Provide Information to the Data Subject: Articles 10 and 11 of directive 95/46/EC, in* THE DATA PROTECTION DIRECTIVE AND MEDICAL RESEARCH ACROSS EUROPE 69-87 (Deryck Beyleveld et al. eds., 2004).

[417] 英國資料保護法 §7；德國聯邦資料保護法 §§ 19 & 34.

[418] 英國資料保護法 §14；德國聯邦資料保護法 §§ 20(1)~(3) & 35.

[419] Directive 95/46/EC Art.14(a); 德國聯邦資料保護法 §20(5).

[420] 英國資料保護法 §13；德國聯邦資料保護法 §7.

[421] Directive 95/46/EC Art.14(b); 英國資料保護法 §11(1).

[422] Directive 95/46/EC Art.15; 德國聯邦資料保護法 §20(5); 英國資料保護法 §12(2)(b).

[423] 值得注意者，我「個資法」並**無規定資料主體得以任何理由，要求資料控制人停止蒐集、處理或利用個資。資料主體須基於法定事由**，例如「正確性有爭議」、「特定目的消失」或「違反本法規定」等，**始得要求資料控制人刪除、停止蒐集、處理或利用**。

[424] 參照「個資法」第 3 條；德國聯邦資料保護法 §6(1).

敏感性個資。公務機關或非公務機關於「敏感性個資之正確性有爭議」、「蒐集特定目的消失屆滿」[425]或「違反本法規定」時，**應主動或依當事人請求**刪除、停止處理或利用。[426]所謂**「違反本法規定」包括違反「個資法」第 6 條禁止蒐集敏感性個資之規定**，此時公務機關或非公務機關應主動或依當事人之請求，刪除、停止蒐集、處理該敏感性個資，且於一定期限內為准駁之決定，並通知當事人。[427]依「個資法」第 12 條規定，公務機關或非公務機關之行為已對本人（當事人）造成侵害者，應查明後以適當方式通知本人（當事人）。此時，本人除得依第 11 條第 4 項請求停止蒐集、處理或利用外，尚得依第 28 條第 1 項（公務機關）或第 29 條第 1 項（非公務機關）向資料控制人請求損害賠償。前者並可附帶請求精神賠償與回復名譽之適當處分。

此外，有關本人「行使拒絕資料控制人蒐集敏感性個資」之方式，「個資法」並無明文規定。查美國「安全港協定」(Safe Harbor Agreements)規定，[428]本人原則上應拒絕資料控制人向第三人揭露或以原始蒐集目的以外之目的，使用本人之個資，例外時以勾選「同意加入」(opt-in)之方式同意；非敏感性個資則反之，原則上同意資料控制人向第三人揭露或以原始蒐集目的以外之目的，使用本人之個資，例外才以勾選「退出」(opt-out)之方式拒絕，亦即向第三人揭露或以原始蒐集目的意外之目的使用敏感性個資，須經本人明確勾選同意，[429]殊值參考。本文認為由

---

[425] 其定義可參見「個資法施行細則草案」第 16 條，係指公務機關經裁撤或改組而無承受業務機關者；非公務機關歇業、解散或所營事業營業項目變更而與原蒐集目的不符者；特定目的已達成而無繼續利用之必要者；其他事由足認該特定目的已無法達成或不存在者。

[426] 參見「個資法」第 11 條第 2 項、第 3 項與第 4 項。

[427] 參見「個資法」第 13 條第 2 項。

[428] 參見 Pricciple 2. Choice

[429] *See* MILLS, *supra* note 137, at 86-87. 美國企業界認為原則上應採用勾選「退出」(opt-out)之方式，且個人接觸權應僅限於敏感性個資，參見 *See* Gregory Shaffer, *Globalization and Social Protection:*

於「個資法」目前並未規定「當事人同意」作為得蒐集敏感性個資之事由，故仿照上開規定提供當事人「同意加入」之方式，以同意資料控制人蒐集敏感性個資之實益不大，故建議直接於本條（第 11 條）新增當事人之拒絕權：

有關第六條第一項所規定資料，當事人得請求公務機關或非公務機關，停止蒐集、處理或利用之。

三、資料品質原則

資料品質原則係指個人資料應確保其正確(accurate)，必要時並更新(up to date)。[430]「個資法」第 11 條第 1 項規定：「公務機關或非公務機關**應維護**個人資料之**正確**，並應主動或依當事人之請求[431]**更正**或**補充**之」。[432]公務機關或非公務機關「蒐集」敏感性個資時，應主動維護資料之正確，發現有誤應主動更正或補充；

The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25 YALE J. INT'L L. 1, 30 (2000). 當事人對於是否勾選「同意加入」(opt-in)，應主動為之，參見 MORGAN & BOARDMAN, *supra* note 120, at 8.3.5.5.

[430] 參照「歐盟個資指令」第 6 條 d 款，惟「歐盟個資指令」之資料品質原則與本文所採之定義並不相同，「歐盟個資指令」之資料品質原則包含甚廣，須予辨明；「OECD 綱領」第 8 條規定，個人資料應與其欲使用之目的相關，並限於該目的之必要範圍，且應確保資料正確(accurate)、完整(complete)與更新(up-to-date) ；英國「資料保護原則」第 4 原則，資料應保持精確(accurate)，必要時並應適時更新(up to date)。其他例如澳洲隱私法「國家隱私原則」第 3 點、「資訊隱私原則」第 3 點與「統一隱私原則」第 9.6 點；德國聯邦資料保護法 § 20(1)；日本個人資料保護法 § 19.

比較法上，本原則存在部分豁免，例如英國資料保護法(§§ 27(3) & (4)(b))將本原則豁免適用「保密條款」。又，比較法上**本項原則係單方面規範資料控制人之義務，並未考量資料主體**。論者以為，本項原則應限縮於「法律明定資料控制人有保護義務」者，或「資料主體具有隱私利益」時，蓋**本原則並未規定適用期間，亦即該資料控制人必須經常性檢視以確保其正確**。參見 *See* 2 ALRC, *supra* note 281, at 27.32 & 34.

[431] 當事人應舉證釋明其之請求，參見「個資法施行細則草案」第 15 條。

[432] *See* 2 ALRC, *supra* note 281, at 27.23.

本人並得藉由行使「個資法」第 10 條與第 11 條之權利，請求公務機關或非公務機關更正或補充敏感性個資。同時，為有助於資料控制人履行「資料品質原則」，資料控制人於蒐集資料時，建議應記載：「該資料係由他人（當事人或第三人）提供之事實」，「確保資料正確性之方法」與「資料更正時聯絡本人之方法」。[433]

四、目的特定原則

「目的特定原則」係指個人資料之「蒐集」應僅限於為（達成）「特定且合法之目的」(specified and lawful purposes)。[434]亦即蒐集之目的，須明確(specified)、合法(lawful)，且該目的須於資料控制人履行「告知義務」時一併告知本人。[435]「個資法」第 15 條規定：「公務機關對個人資料之**蒐集**或處理，**除第六條第一項所規定資料外，應有特定目的…**」；第 19 條規定：「非公務機關對個人資料之**蒐集**或處理，**除第六條第一項所規定資料外，應有特定目的…**」，皆為「目的特定原則」之體現。

猶需注意者，上開規定明文排除第 6 條第 1 項之敏感性個資，其用意在使公務機關或非公務機關逕依第 6 條第 1 項但書之規定，以蒐集敏感性個資，[436]並非

---

433 *See* JOHN MACDONALD QC & CLIVE H. JONES (EDS.), *supra* note 337, at 10.30.

434 參見英國資料保護法附表一第一部份第二點；澳洲隱私法「國家隱私原則」第 2 點、「資訊隱私原則」第 9 點；「歐盟個資指令」第 6 條 b 款規定，蒐集資料之目的應特定(specified)、明確(explicit)、合法(legitimate)，且不得使用於與原始蒐集目的顯不相容(incompatible)之情形；「OECD 個資綱領」第 9 條規定，個人資料之蒐集目的應於蒐集時明確指定；其後續使用限於達成該目的，或其他與原始目的非不相容且於各該變更時即明確指定者。

435 *See* JOHN MACDONALD QC & CLIVE H. JONES (EDS.), *supra* note 337, at 10.28. 此涉及告知義務與告知事項之問題，下詳。

436 依 2009 年 11 月 12 日「立法院朝野黨團協商結論」，於「個資法」第 15 條與第 19 條新增「除第六條第一項所規定資料外」之用語，其修正說明謂：「本條僅適用於一般個人資料，特種資料之蒐集或處理，仍應依本法第六條規定為之」，參見立法院公報，99 卷 29 期，頁 376。

認為「蒐集敏感性個資無須有特定目的」；且遍查英、德、澳洲有關「目的特定」之規定，並無明文排除「敏感性個資」者，故**公務機關或非公務機關蒐集敏感性個資時，仍應有特定目的**，建議將第 15 條與第 19 條所謂「除第六條第一項所規定資料外」之文字，移至同項後段。第 15 條修正為：

> **「公務機關對個人資料之蒐集或處理，應有特定目的。除第六條第一項所規定資料外，應符合下列情形之一者：…」；**

第 19 條修正為：

> **「非公務機關對個人資料之蒐集或處理，應有特定目的。除第六條第一項所規定資料外，應符合下列情形之一者：…」**

蒐集之目的，是否因敏感性個資而須受有限制，查法國資料保護法規定：蒐集、處理或利用敏感性個資之目的，須與「例外得蒐集、處理或利用」之規定相符，此即為「目的限制」(purpose-limitation)；[437]「澳洲法改會」(Australian Law Reform Commission, ALRC)認為：藉由「例外得蒐集敏感性個資」之規定，將得以確保蒐集敏感性個資之目的係屬合理(reasonable)。[438]綜上，**公務機關或非公務機關蒐集（處理或利用）敏感性個資之目的，須符合「個資法」第 6 條第 1 項但書所訂之四款要件之一**，例如公務機關為履行其法定職務而須蒐集他人之健康記錄時，該公務機關之「蒐集目的」須為「履行其法定職務」。又，資料控制人嗣後變更使用目的，[439]一般屬「利用限制」之問題，蓋資料係已到手，而非資料尚留待於本人

---

[437] *See* Korff, *supra* note 31, at 87; 法國資料保護法 § 8(2).

[438] *See* 2 ALRC, *supra* note 281, at 21.77.

[439] 特定目的之消失或屆滿，其定義可參見「個資法施行細則草案」第 16 條。

手中，本章第四節後詳。

五、責任歸屬原則

「責任歸屬原則」係指：資料控制人(data controller)有責任遵守相關措施，以實踐上開各項個人資料保護原則。依「個資法」之規定，公務機關或非公務機關「蒐集」敏感性個資時，應遵循之個人資料保護原則，有如下各條：

1. 第 5 條（依誠實信用方法蒐集個資，並尊重本人權益）；
2. 第 6 條（符合得蒐集敏感性個資之情形）；
3. 第 8 條（直接蒐集之告知義務）或第 9 條（間接蒐集告知義務）；
4. 第 10 條（答覆本人請求）；
5. 第 11 條（確保資料正確，並更正或補充本人之敏感性個資）；
6. 第 12 條（致生損害時應通知本人）；
7. 第 15 條（公務機關蒐集敏感性個資應有特定目的）或第 19 條（非公務機關蒐集敏感性個資應有特定目的）。

第三節　敏感性個資之「處理」相關原則

本節討論公務機關或非公務機關「處理」敏感性個資時，應遵循之個人保護原則。所謂「處理」，依「個資法」第 2 條第 4 款規定，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**。公務機關或非公務機關「處理」敏感性個人資料時，除應尊重當事人之權益，並使用誠實及信用方法外，[440]其「處理」之行為，尚須符合「個資法」第 6 條第 1 項但書各款之要件。

一、個人參與原則

「個人參與原則」之概念，已如前述。依「個資法」第 10 條規定，本人得向公務機關或非公務機關查詢其所「處理」之敏感性個資。公務機關或非公務機關於「敏感性個資之正確性有爭議」或「違反本法規定」時，**應主動或依當事人請求**刪除、停止處理之。[441]所謂**「違反本法規定」包括違反「個資法」第 6 條禁止處理敏感性個資之規定**，此時公務機關或非公務機關應主動或依當事人之請求，刪除、停止處理該敏感性個資，且於一定期限內為准駁之決定，並通知當事人。[442]如公務機關或非公務機關之行為已對當事人造成侵害者，應查明後以適當方式通知當事人，[443]當事人並得請求損害賠償。[444]

---

[440] 參照「個資法」第 5 條。

[441] 參見「個資法」第 11 條第 2 項、第 3 項與第 4 項。

[442] 參見「個資法」第 13 條第 2 項。

[443] 參見「個資法」第 12 條。

[444] 參見「個資法」第 28 條第 1 項與第 29 條第 1 項。

二、資料品質原則

「資料品質原則」之概念，已如前述。依「個資法」第 11 條第 1 項規定，公務機關或非公務機關**應維護**個人資料之**正確**，並應主動或依當事人之請求[445]**更正**或**補充**之」。[446]公務機關或非公務機關如於「處理」敏感性個資時，發現疑似缺誤而欲更正或補充，此時可藉由「蒐集」敏感性個資時，已明確載明之「聯絡本人之方法」，主動聯絡本人以確認該資料之正確。

三、目的特定原則

有關資料控制人「處理」個資之「目的特定原則」，係指資料控制人不得以「與原始蒐集目的不相容」之方式(in any manner incompatible with that purpose)，處理其個人資料。「個資法」第 5 條規定：「個人資料之蒐集、**處理**或利用，應尊重當事人之權益，依誠實及信用方法為之，**不得逾越特定目的**之必要範圍，並應與**蒐集之目的具有正當合理之關聯**」；第 15 條規定：「公務機關對個人資料之蒐集或**處理…應有特定目的…**」；第 16 條規定：「非公務機關對個人資料之蒐集或**處理…應有特定目的…**」，皆為「目的特定原則」之體現。公務機關或非公務機關「處理」敏感性個資時，其目的仍應符合「蒐集目的之必要範圍」，亦即**符合「個資法」第 6 條第 1 項但書所訂之四款要件之一**，理由已如前述。此外，為確保本原則之落實，主管機關執行業務檢查而認有必要或有違反本法之虞時，應檢視公務機關或非公務機關是否僅於特定目的內「處理」個人資料。[447]至於有無逾越特定目的，應採「合理客觀」之觀點予以判斷。[448]

---

[445] 當事人之請求應舉證釋明，參見「個資法施行細則草案」第 15 條。

[446] *See* 2 ALRC, *supra* note 281, at 27.23.

[447] 參照「個資法」第 22 條。

[448] *See* 1 ALRC, *supra* note 32, at 21.73.

此外，資料之處理仍應與處理目的「適當」(adequate)、「相關」(relevant)且「不過度」(not excessive)。[449]所謂「適當」指資料控制人應完成其處理目的之必要工作，例如信用貸款審核之資料控制人，發現資料內記載資料主體現正與他人進行民事訴訟，此時資料控制人應登載該訴訟是否已終結或執行完畢；[450]所謂「相關」須取決於資料「處理之目的」，例如建立個人之工作履歷時，可登載本人之「健康資訊」，但不可登載本人之「基因資訊」，蓋「基因資訊」與工作履歷幾無相關；所謂「不過度」，係避免在未來任何期間內，以任何不確定之方法處理該資料，以增加資料外洩的風險。為避免過度處理個資，英國資料保護署(The Information Commissioner's Office, ICO)建議，資料控制人於蒐集敏感性個資時，蒐集資料之數量應盡量減少，可茲參考。[451]

四、公開原則

「個資法」第 17 條規定，**公務機關**應將：「個人資料**檔案名稱**」、「保有**機關名稱及聯絡方式**」、「個人資料檔案保有之**依據及特定目的**」及「個人資料之**類別**」公開於電腦網站，或以其他適當方式供公眾查閱，其有變更者亦同，此為「公開原則」。[452]「公開原則」所要求者，係資料控制人應將其處理資料之實踐「透明化」

---

[449] 英國資料保護法附表一第一部份第三點。英國資料保護署將本原則與「資料品質原則」、「期間限制原則」合併稱為「個人資訊標準」(information standards)，參見 UK ICO, *supra* note 382, at 57.

[450] *See* MACDONALD QC & JONES (EDS.), *supra* note 337, at 10.29.

[451] *See* UK ICO, *supra* note 382, at 60.

[452] 澳洲隱私法「國家隱私原則」第 5 點、「資訊隱私原則」第 5.1 點；「OECD 綱領」第 12 條規定，關於個人資料之發展(developments)、實踐(practices)及政策(policies)，應有普遍性之公開政策。個人資料之存在(existence)、性質(nature)、主要使用目的、資料控制人之身分(identity)及日常住所，應使用合宜之方法以供公眾確認。英國與德國之立法未有此公開原則，蓋英國要求資料控制人處理個人資料前，須向主管機關 ICO 進行登記，其登記之內容與公開原則所要求者，

(transparent)，[453]而不是將其「處理之過程」一律公開。此原則與「告知義務」在概念上有所重疊。[454]

公務機關處理敏感性個資時，除須**依法公開前揭事項**外，**應於說明「個人資料檔案保有之依據及特定目的」時，須附帶註明其適用「個資法」第 6 條第 1 項但書之條款**，並避免揭露本人之身分。值得注意者，上開條文僅適用「公務機關」，未及於「非公務機關」。本文認為，基於非公務機關之人員配置與成本考量，要求「非公務機關」比照「公務機關」履行上開規定，實行上將有困難，茲參考澳洲隱私法，[455]**建議「非公務機關」應以適當方式公開其「隱私政策」**(Privacy Policies)，[456]**主動說明其管理**(management)**個人資料之方法**。

五、安全保障原則

「個資法」第 18 條規定：「公務機關保有個人資料檔案者，應**指定專人辦理安全維護事項**，防止個人資料被竊取、竄改、毀損、滅失或洩漏」；第 27 條第 1 項規定：「非公務機關保有個人資料檔案者，應**採行適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏」，此為「個人資料保護原則」之「安全保障

幾無差異(§ 16)；德國同樣要求資料控制人，於進行自動化之處理程序前，須向主管機關進行登記(§§ 4d & 4e)。「澳洲法改會」建議應公開：資料之性質；持有各類型資料之目的；資料當事人之類型；持有各類資料之期間；何人於何種情形下應如何接觸該資料。此外，**資料控制人若依法可拒絕他人接觸該個人資料時，將無須適用本項原則**，參見 1 ALRC, *supra* note 32, at 24.3.

[453] *See* 1 ALRC, *supra* note 32, at 24.1

[454] 本原則所要求者為向「**不特定多數人**」公開，而資料控制人之告知義務係以**資料當事人為「特定人」**，參見 1 ALRC, *supra* note 32, at 24.10 & 24.11.

[455] 澳洲隱私法「國家隱私原則」第 5 點。

[456] 「澳洲法改會」認為「私人機構之隱私政策」應公開：是否持有(possession)或控制(control)個人資料；個人資料之性質(nature)、使用(used)之目的與接觸個人資料之方法，參見 1 ALRC, *supra* note 32, at 24.14.

原則」。[457]所謂「安全維護事項」或「適當安全措施」，按「個資法施行細則草案」第 9 條第 1 項，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必要措施**。同條第 2 項詳細規定「必要措施」之內容。[458]此外，前開規定雖同樣要求公務機關或非公務機關須制定安全保護措施，惟僅公務機關須「指定專人」辦理，非公務機關則無此義務，此應為考量非公務機關之編制與成本所為之規定，但對非公務機關而言，負責保管資料之人常為非專業之保管人，例如負責掌管視聽配備或檔案櫃者，此時該資料即有洩漏之虞，[459]故非公務機關於擬定保護措施時，應審慎考量「保管人之能力」以建立適合之保護措施。非公務機關違反本項規定以致資料洩漏或致使他人受有損害，須負損害賠償責任。[460]

上開條文適用之客體為「個人資料」，解釋上當然包含敏感性個資，但是因為敏感性個資之性質，其不當外洩將嚴重侵害個人權利，所以是否須針對敏感性個資，另訂更嚴格之安全維護措施，仍值研究。查各國立法例，似未有針對敏感性個資之特殊安全維護措施規定。歐盟理事會(Council of Europe) 建議：「歐盟個資

---

[457] 英國資料保護法附表一第一部分第 7 點；日本個人資料保護法 §§ 20 & 21; 「OECD 綱領」第 11 條。

[458] 「個資法施行細則草案」第 9 條第 2 項：「前項必要措施，應包括下列事項：一、成立管理組織，配置相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、必要之使用紀錄、軌跡資料及證據之保存。十一、個人資料安全維護之整體持續改善。

[459] *See* DAVID G. HILL, DATA PROTECTION: GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 9.3.2 (2009).

[460] 此時本人除可依「個資法」第 29 條向非公務機關請求損害賠償外，或可依民法第 184 條第 2 項違反保護他人法律之情形，訴請賠償，參見侯英泠，〈醫療機構、外科醫師與麻醉科醫師之說明義務〉，《台灣法學雜誌》，107 期，頁 296（2008 年 6 月）。

公約」所定義之敏感性個資，不得單獨儲存或與其他第三人可接觸之資料共同儲存；[461]「APEC隱私保護綱領」第 22 點規定，資料控制人所採取之保護措施，應與**濫用行為之發生機率、可能造成之傷害、個人資料之敏感度**和**內容**合乎比例，並應定期檢視和重新評估保護措施。[462]在未確保資料安全之情形下，將有可能發生身份竊盜 [463]等違法情事。加拿大「個人資料與電子文件保護法」(Personal Information Protection and Electronic Documents Act, PIPEDA)規定，私人機構應針對性質較為敏感(sensitivity)之資料提供適當保護措施；[464]英國資料保護署(The Information Commissioner's Office, ICO)建議，決定「適當安全措施」時應考量：資料之**性質**（是否具有價值、敏感性或信賴關係）與其遭誤用或意外洩漏時，對當事人**可能產生之傷害**後，再斟酌該組織之能力、電腦系統情況、雇員數量、儲存資料多寡，以及他人是否以機關之名義持有資料等事項，進行風險評估以決定適當安全措施。[465]以上各國經驗，大多建議資料控制人**應考量「資料之性質（敏感性）」與「對本人可能造成之傷害」以決定適當安全措施**。[466]本文建議，「個資法

[461] Appendix to Recommendation No. R (91) 10 3.1 (“Personal data falling within any of the categories referred to in Article 6 of Convention No. 108 should not be stored in a file or in part of a file generally accessible to third parties.”)

[462] APEC Privacy Framework Principle VII 22.

[463] 係指未經授權使用個人之姓名、生日，社會安全號碼以獲取銀行信用卡、貸款與帳戶資訊，相關討論可參見 1 ALRC, *supra* note 32, at 473-482.

[464] 參見加拿大個人資料與電子文件保護法附表一第 4.7 點原則 7。

[465] 適當安全措施又可依機關、機構內之對象，分為管理與經營措施、雇員訓練、物理性安全維護與電腦安全。所謂「管理與經營措施包括建立身份識別與授權制度，並清楚劃分掌管資料之職權與政策；雇員訓練包括提升其對個人資料保護法之理解；物理性安全維護則指儲存檔案之處所安全，包括檔案系統、電腦硬體、門禁出入管制等；電腦安全則指系統軟體方面，一般常見者為進行加密。參見 *See* UK ICO, *supra* note 382, at 85-88.

[466] 鑑於科技之發展，蒐集方式已不限於傳統之「直接蒐集」與「間接蒐集」，參見本章第二節之討論。隸屬德國聯邦資料保護法底下，負責電信工作事務之組群「柏林小組」(Berlin Group)認為，以網路傳輸敏感性個資時，應予加密，參見 Reidenberg, *supra* note 119, at 1359 n.242. 歐盟執委會亦認為：使用 RFID 技術時，其安全維護措施同樣應予提高，

施行細則草案」[467]可針對敏感性個資「適當安全措施」，增訂：

公務機關或非公務機針對第六條第一項所規定之資料，採取技術上及組織上之必要措施時，應考量資料之性質與對本人可能造成之傷害。

近日，行政院宣布將建構「醫療雲端運算系統」[468]，以儲存個人醫療資料。有學者認為應禁止將敏感性個資儲存於雲端技術，以免資料外洩。[469]本文認為，建構「雲端運算系統」時，應確保該個人醫療資料完全「匿名化」使不可辨識資料本人，且須提升適當安全措施，以防有心人士，例如藥廠、研究單位或保險公司等未經許可之使用。此外，本「醫療雲端運算系統」若無法律明文規定設置或非屬公務機關之法定職務，而屬「個資法」第 6 條第 1 項但書第 4 款（公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序者）者，有關「醫療資料」之蒐集、處理與利用之「範圍」、「程序」與其他「應遵行事項」，應符合中央目的事業主管機關與法務部共同訂定之辦法（參照第 6 條第 1 項）。

六、期間限制原則

我「個資法」未特別規定資料之「期間限制」。所謂「期間限制」係指儲存之

---

[467] 參見「個資法施行細則草案」第 9 條第 1 項。

[468] 中時電子報，〈醫療雲洩個資 消基會擬打團體訴訟〉，最後瀏覽日期 2012/02/25，網址：http://tw.news.yahoo.com/%E9%86%AB%E7%99%82%E9%9B%B2%E6%B4%A9%E5%80%8B%E8%B3%87-%E6%B6%88%E5%9F%BA%E6%9C%83%E6%93%AC%E6%89%93%E5%9C%98%E9%AB%94%E8%A8%B4%E8%A8%9F-213000193.html

[469] *See* Gurpreet Dhillon & Ella Kolkowska, *Can a Cloud Be Really Secure? A Socratic Dialogue*, *in* COMPUTERS, PRIVACY AND DATA PROTECTION: AN ELEMENT OF CHOICE 348 (Serge Gutwirth, Yves Poullet, Paul De Hert & Ronald Leenes eds., 2010).

個人資料，其蒐集及處理**不得逾越原始目的之必要期間**，[470]此原則與「目的特定原則」與「安全保障原則」意義上有部分重疊。儲存過久之個人資料，將提高誤用的風險，且隨著期間增加，越難確保該資料之正確性，也增加回應當事人請求接觸之困難。[471]此時，資料控制人應審視儲存之個人資料期間與原始目的，將不再需要之個人資料安全刪除，並更新之。[472]關於期間之長短，原則上應取決於個案事實，[473]資料控制人應考量：該資料於現實或未來之價值；保有該資訊之利益、風險與負擔；確保該資料正確（即履行資料品質原則）之難易度。[474]例如受雇人離職後，雇用人應刪除其依法提供健康檢查之資料。雇用人於接受應徵申請時，亦不得保留應徵者之申請資料，超過必要期間。

我國「個資法」雖未就特別限制資料之儲存期間，解釋上，資料控制人儲存個資之期間仍應以「完成特定目的之必要範圍」為限。[475]一般而言，以研究為目的所儲存之個人資料，較有可能違反本項原則。[476]公務機關或學術研究機構依「個資法」第 6 條第 1 項但書第 4 款處理敏感性個資者，須注意中央目的事業主管機關，根據其「範圍」、「程序」與「應遵行事項」訂定之辦法。[477]此外，其他現行法，則對部分敏感性個資訂有儲存期間之限制，例如：

1. 醫療法(100/12/21)第 70 條（病歷應至少保存 7 年，惟人體試驗之病歷，

---

[470] 英國資料保護法(Sch.1 Part I 5)；澳洲隱私法「國家隱私原則」第 4 點；德國聯邦資料保護法§§ 20(2)2 & 35(2)3; Directive 95/46/EC Art. 6(e).

[471] *See* UK ICO, *supra* note 382, at 73.

[472] *See id.*

[473] *See* MACDONALD QC & JONES (EDS.), *supra* note 337, at 10.31.

[474] *See* UK ICO, *supra* note 382, at 74.

[475] 參照「個資法」第 5 條。

[476] *See* MACDONALD QC & JONES (EDS.), *supra* note 337, at 10.31.

[477] 參照「個資法」第 6 條第 2 項。

應永久保存）。

2. 去氧核醣核酸採樣條例(101/01/04)第 12 條第 1 項與第 2 項（去氧核醣核酸之樣本至少應保存 10 年，去氧核醣核酸之紀錄至少應保存至被採樣人死亡後 10 年；符合特定條件時，主管機關「應」刪除其資料，被採樣人亦「得」申請刪除之）。

上開法律並未規定公務機關或非公務機關應於何時刪除或排除該敏感性個資。本文以為，公務機關或非公務機關於上開**期限屆滿時**，應主動刪除敏感性個資，本人亦得根據「個資法」第 10 條規定，向公務機關或非公務機關查詢其所「處理」之敏感性個資。其餘未訂定處理期間之敏感性個資，公務機關或非公務機關則須注意前述判準要點，於該資料**符合之「特定目的」結束時**，安全刪除之。

七、責任歸屬原則

「責任歸屬原則」係指：資料控制人有責任遵守相關措施，以實踐上開各項個人資料保護原則。依「個資法」之規定，公務機關或非公務機關「處理」敏感性個資時，應遵循之個人資料保護原則，有如下各條：

1. 第 5 條（依誠實信用方法處理個資，並尊重本人權益）。
2. 第 6 條（符合得處理敏感性個資之情形）。
3. 第 10 條（答覆本人請求）。
4. 第 11 條（確保資料正確，並更正或補充本人之敏感性個資）。
5. 第 12 條（致生損害時應通知本人）。
6. 第 15 條（公務機關處理敏感性個資應有特定目的）或第 19 條（非公務機關處理敏感性個資應有特定目的）。
7. 第 17 條（公務機關應主動公開相關事項）。

8. 第 18 條（公務機關指定專人辦理安全維護措施）；第 27 條（非公務機關應採行適當安全措施）。

第四節　敏感性個資之「利用」相關原則

本節討論資料控制人於「蒐集」、「處理」敏感性個資後，進行「利用」時應遵循之個人資料保護原則。所謂「利用」，按「個資法」第 2 條第 5 款，係指**將蒐集之個人資料為處理以外之使用**。公務機關或非公務機關「利用」敏感性個人資料時，除應尊重當事人之權益，並使用誠實及信用方法外，[478]其「利用」之行為，尚須符合「個資法」第 6 條第 1 項但書之規定。以下分項討論各種個人資料保護原則。

一、個人參與原則

「個人參與原則」之概念，已如前述。依「個資法」第 10 條規定，本人得向公務機關或非公務機關查詢其所「利用」之敏感性個資。公務機關或非公務機關於「敏感性個資之正確性有爭議」或「違反本法規定」時，**應主動或依當事人請求**刪除、停止利用之。[479]所謂**「違反本法規定」包括違反「個資法」第 6 條禁止利用敏感性個資之規定**，此時公務機關或非公務機關應主動或依本人（當事人）之請求，刪除、停止利用該敏感性個資，且於一定期限內為准駁之決定，並通知本人（當事人）。[480]如公務機關或非公務機關之行為已對當事人造成侵害者，應查明後以適當方式通知當事人，[481]當事人並得請求損害賠償。[482]

---

[478] 參照「個資法」第 5 條。

[479] 參見「個資法」第 11 條第 2 項、第 3 項與第 4 項。

[480] 參見「個資法」第 13 條第 2 項。

[481] 參見「個資法」第 12 條。

[482] 參見「個資法」第 28 條第 1 項與第 29 條第 1 項。

二、資料品質原則

「資料品質原則」之概念，已如前述。依「個資法」第 11 條第 1 項規定，公務機關或非公務機關**應維護**個人資料之**正確**，並應主動或依當事人之請求[483]**更正**或**補充**之。[484]資料控制人利用敏感性個資時，須注意資料之正確性，例如公務機關或非公務機關使用本人之「生物辨識資訊」作為門禁系統辨識用途，當該系統無法辨識出本人之身分時，該管機關或機構即有違背本項原則之虞。[485]

三、目的特定原則

有關資料控制人「利用」個資之「目的特定原則」，係指資料控制人僅得於「原始蒐集目的內」利用個人資料。[486]我「個資法」第 5 條規定：「個人資料之蒐集、處理或**利用**，應尊重當事人之權益，依誠實及信用方法為之，**不得逾越特定目的**之必要範圍，並應與**蒐集之目的具有正當合理之關聯**」；第 16 條規定：「公務機關對公務機關對個人資料之**利用，除第六條第一項所規定資料外，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**…」；第 20 條規定：「非公務機關對個人資料之**利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內**為之…」，皆為「目的特定原則」之體現。

上開條文所稱「第六條第一項所規定資料」係指敏感性個資，「個資法」第 16

---

[483] 當事人應舉證釋明其請求，參見「個資法施行細則草案」第 15 條。

[484] *See* 2 ALRC, *supra* note 281, at 27.23.

[485] *See* 1 ALRC, *supra* note 32, at 10.74.

[486] 「APEC 隱私框架」第 4 點：個人資料之利用僅限於與蒐集目的一致或相關的範圍內，但有下列情況，不在此限：a) 取得當事人本人的同意；b) 為提供當事人所要求之產品或服務所必要者；或 c) 法律明文規定者；澳洲隱私法「國家隱私原則」第 2 點與「資訊隱私原則」第 9 至第 11 點。

條與第 20 條排除敏感性個資，其用意在使公務機關或非公務機關逕依第 6 條第 1 項但書之規定利用敏感性個資，[487]惟此一立法方法是否妥適，仍值商榷。蓋第 6 條第 1 項後段文字，**所規定者為「豁免禁止，得利用敏感性個資之情形」，未有任何有關個資利用目的之原則性宣示**，如此規定易使人誤以為：利用敏感性個資僅須符合第 6 條第 1 項但書規定，而其利用目的不必與原始蒐集目的相符，或其利用行為不限於原始蒐集目的之必要範圍內。此作法等同將敏感性個資移置個人資料保護原則（利用限制）以外，違背加強保護敏感性個資之宗旨。即便透過解釋，認為「第六條第一項所規定資料」之文字，僅在排除適用條文後段所謂「目的外利用」之情形，上開文字也應該改置於本條但書前段，以第 16 條為例，應改為：「公務機關對公務機關對個人資料之利用，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，**除第六條第一項所規定資料外，得為特定目的外之利用」**，惟此移置文字之作法，卻會使但書之情形（二次目的之利用）不適用於敏感性個資。綜上，本文認為，公務機關利用敏感性個資，仍應「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」；非公務機關利用敏感性個資，應「於蒐集之特定目的必要範圍內」為之，建議修法將第 16 條與第 20 條「**除第六條第一項所規定資料外」之文字予以刪除**。

四、利用限制原則

前揭「目的特定原則」宣示：資料控制人利用敏感性個資之目的應予特定，且**與蒐集之特定目的相符**，此為「原始蒐集目的內」之利用，至於「原始蒐集目的外」之利用，則屬於「特定（蒐集）目的外之利用」或「二次目的」之問題，須符合法定要件始得為之。「個資法」第 16 條但書後段與第 20 條第 1 項但書後段

[487] 依 2009 年 11 月 12 日「立法院朝野黨團協商結論」，於「個資法」第 15 條與第 19 條新增「除第六條第一項所規定資料外」之用語，其修正說明謂：「**本條僅適用於一般個人資料，特種資料之蒐集或處理，仍應依本法第六條規定為之**」，參見立法院公報，99 卷 29 期，頁 376。

分別規定公務機關與非公務機關得進行之二次目的利用之情形。至於敏感性個資之二次目的利用，是否須適用上開條文，本文持肯定見解，[488]故**公務機關與非公務機關進行敏感性個資「二次目的之利用」時，須先符合「個資法」第 6 條第 1 項但書之一規定，繼而適用第 16 條或第 20 條第 1 項之「二次目的」規定**，例如公務機關或學術研究機構依第 6 條第 1 項但書第 4 款（公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料）利用敏感性個資時，得依上開第 16 條第 5 款（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）或第 20 條第 5 款（要件與前款相同[489]），進行二次目的之利用。此外，敏感性個資如得以進行「二次目的之利用」時，公務機關與非公務機關是否須再次履行「通知義務」，「個資法」未有明文。本文以為，為徹底符合「利用限制原則」與「告知義務」，公務機關與非公務機關以「二次目的」利用本人之敏感性個資時，應主動通知本人。[490]有關敏感性個資之「二次目的之利用」，茲有以下疑問。

（一）利用敏感性個資之二次目的，是否與原蒐集目的須「直接相關」？

敏感性個資之處理及利用，固然須符合「目的特定原則」，惟利用目的變更後，「原始蒐集目的」與「二次目的」之間是否有關連性，則不無疑問。查澳洲「隱私法」規定，私人機構使用或揭露(use and disclosure)敏感性個資之目的，與原先蒐集目的不同時，其**使用或揭露敏感性個資之目的與原先蒐集之目的必須「直接**

---

488 不同意見，參見林秀蓮，〈個人資料保護法初探〉，《萬國法律》，頁 3（2011 年 4 月）。

489 猶須注意者，本條所規範主體為「非公務機關」於特定目的外利用個資之情形，惟本款豁免限制之主體卻為「公務機關或學術研究機構」，將形成「非公務機關」使用「經公務機關或學術研究機構處理之匿名化個資」，以進行二次目的利用之情形。

490 *See* MORGAN & BOARDMAN, *supra* note 120,at 8.3.5.6

相關」(directly related)；且**本人對資料控制人所進行之二次目的利用行為應有「合理期待」**(reasonable expect)。[491]一般而言，一般個人資料因其揭露或使用造成傷害之風險相對較低，所以原始蒐集目的與變更後之二次目的，兩者目的間無須以具有「直接相關」為限；惟敏感性個資因其性質特殊，易對資料主體造成隱私侵害，故二次目的之利用須謹慎小心，其原始蒐集目的須與二次目的有「**直接相關**」為要。[492]例如醫師基於保險理賠之目的，向保險人（例如中央健保局）揭露病人之健康資訊者，該目的應與蒐集資料之主要目的－診療病人屬於直接相關，[493]且病人對於醫師向保險業者揭露其個人資料之行為，應有合理期待。[494]本文認為，「合理期待」事涉資料當事人之主觀想法，難以要求資料控制人確實遵循，故仍應以「直接關連」作為判斷基準，較為明確。

（二）利用敏感性個資之二次目的，是否及於「行銷」？

「個資法」第 20 條第 2 項規定：「非公務機關依前項規定利用個人資料行銷者，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」；第 3 項規定：「非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用」。上開兩者為當事人拒絕（行銷）權。[495]根據第 20 條第 2 項規定，當事

---

[491] 參見澳洲隱私法「國家隱私原則」第 2.1(a)項。合理期待之概念應以通念理解，並參考資料是否具有高度敏感性，參見 2 ALRC, *supra* note 281, at 25.39 & 26.83.

[492] *See* 澳洲隱私法「國家隱私原則」第 2.1(a)(i)項； 2 ALRC, *supra* note 281, at 25.50.

[493] *See* 2 ALRC, *supra* note 281, at 25.145.

[494] 澳洲隱私法「統一隱私原則」第 5.1(a)點。雇用人如欲以「二次目的」使用或揭露受雇人之敏感性個資，且該目的與原始蒐集目的無「直接」相關，其使用或揭露並不屬當事人合理期待者，則須獲得當事人之同意。*See* 2 ALRC, *supra* note 281, at 40.118.

[495] 「歐盟個資指令」Art.14(b)；英國資料保護法 § 11.

人得拒絕非公務機關利用敏感性個資以進行行銷。惟此仍有賴當事人主動提出，[496]當事人未拒絕時，非公務機關仍得以「行銷」作為二次目的，利用敏感性個資，例如醫院外科替病患切除肢體後，將病患之資料交由整形科來進行行銷。查澳洲隱私法規定，**禁止以「行銷」為二次目的，使用或揭露**(use and disclosure)**敏感性個資**。[497]資料控制人如欲以敏感性個資進行行銷，該資料之原始蒐集目的須為「行銷」或與「行銷」直接相關。[498]「澳洲法改會」(Australian Law Reform Commission, ALRC)建議，以敏感性個資進行行銷者，須限於「具有合理期待之現有顧客關係」(existing customer)。[499]本文認為，基於敏感性個資之性質，不當利用將侵害個人隱私，建議修法限縮敏感性個資之二次目的利用，於「個資法」第 16 條新增第 2 項為：

「公務機關利用第六條第一項所規定之資料進行特定目的外之利用，其特定目的與原始蒐集目的應直接相關」；

第 20 條新增第 4 項為：

「非公務機關利用第六條第一項所規定之資料進行特定目的外之利用，其特定目的與原始蒐集目的應直接相關，且不得利用該資料行銷。

---

[496] 一般認為，非公務機關應提供勾選「退出」(opt-out)來代替書面同意，參見王郁琦、陳炳全，〈濫發網際網路廣告信相關法律問題之研究〉，《月旦法學》，81 期，頁 156（2002 年 2 月）。本文認為，資料涉及敏感性資訊時，仍應以「同意加入」(opt-in)之方式規範為宜。

[497] 參見澳洲隱私法「國家隱私原則」第 2.1(c)點。

[498] 其他例如取得當事人之同意，亦得使用或揭露敏感性個資為行銷之用，參見 *See* 2 ALRC, *supra* note 281, at 26.83. 澳洲隱私法(NPPs 2.1(c))規定，資料控制人基於當事人之同意或該資料非屬敏感性個資且使用或揭露前，向當事人取得同意係顯不可行者(impracticable)，得為二次目的使用或揭露之。

[499] *See* 2 ALRC, *supra* note 281, at 26.83 & 26.84. 現存顧客關係係指正在進行中之商業、契約或營業關係，應參酌個別情況單獨判斷之。

五、國際傳輸

按「個資法」第 2 條第 6 款規定，「國際傳輸」，係指將個人資料作跨國（境）之處理或利用。同法第 21 條規定，「**非公務機關**為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：一、涉及國家重大利益。二、國際條約或協定有特別規定。三、接受國對於個人資料之保護**未有完善之法規**，致有損當事人權益之虞。四、以迂迴方法向第三國（地區）傳輸個人資料規避本法」。

現時網路科技發展進步，各類型之個人資料常流通於跨國私人機構中，惟各國個人資料保護層級不一，常見在A國受保護之資料，傳遞自B國不受保護之情形。因此，多數國家禁止向未提供資料保護之國家傳輸資料。例如 1989 年法國資料主管機關便禁止飛雅特(Fiat)法國公司向義大利分公司傳送個人紀錄，因為當時義大利尚未制定個人資料保護法，而法國卻已有相當高的保護水平；[500]「歐盟個資指令」第 25 條規定，各會員國不得將資料傳往未提供適當保護水平之國家。[501]美國為確保私人企業之商業利益，由商務部(U.S. Department of Commerce)制訂「安全港協定」(U.S.-EU Safe Harbor Agreements)[502]，以解決歐盟與美國個人資料保護立法之歧異。上開例示規定，皆為防止個人資料傳往其他未提供適當保護水平國家。

我國非公務機關欲向其他國家傳輸個人資料時，須注意該接受國是否對個人

---

[500] *See generally* Peter Mei, *The EC Proposed Data Protection Law*, 25 L. & POL'Y INT'L BUS. 305-34 (1993).

[501] Directive 95/46/EC Art.25(4); 英國資料保護法(Sche.1 Part I 8); 德國聯邦資料保護法 §4b(2)；澳洲隱私法「國家隱私原則」第 9 點。有關跨國資料保護之必要性，可參見陳榮傳，〈再論資料跨國流通〉，《月旦法學》，78 期，頁 165-177（2001 年 11 月）。

[502] International Safe Harbor Privacy Principles, *available at* http://www.ita.doc. gov/ecom/shprin.html (last visited Feb. 10, 2012).

資料有「完善保護法規」。所謂「完善保護法規」,「個資法」與「個資法施行細則草案」並未定義，除須視接受國是否制訂個人資料保護法外，應考慮：「資料之性質、處理目的、持續時間等」。[503]國際傳輸敏感性個資時，尚須注意：敏感性個資之類別是否同屬該國特別保護之個資，且得蒐集、處理或利用之要件，是否符合該國之法規規定。

「個資法」並未定義國際傳輸之「接受國」。事實上，藉由電子郵件或網站公開等方式傳遞資料，很有可能使個人資料「路經」他國。例如A國醫師將有關病人之健康檢查資訊傳給住在A國的病人，但其使用的郵件系統隸屬美國微軟公司，其伺服器資料庫只要設於非屬A國之海外，該醫師之行為即構成國際傳輸。[504]惟此理解似偏重形式，如將所有資料傳遞之過程檢視，而無視他人是否得以接觸該資料，國際傳輸之規範將治絲益棼，徒增困擾。本文以為，可參考澳洲「法改會」(Australian Law Reform Commission, ALRC)建議，考量**本國以外之地區，是否可以接觸**(access)**或檢視**(view)**該資料**，作為認定「接受國」之標準。如他人得在本國以外其他地區接觸或檢視該資料，則該地區則屬資料之「接受國」，[505]故上開例示並不構成違反國際傳輸原則。[506]

國際傳輸敏感性個資時，是否應適度加強安全維護措施，各國立法例似無明文規定，英國資料保護署(Information Commissioner's Office)建議：資料控制人可考慮將資料匿名化或編碼化。[507]本文建議，可參考前揭「安全保障原則」，考量「資

---

[503] 德國聯邦資料保護法 §4b(3)；英國資料保護法(Sche.1 Part II 13)。

[504] *See* 2 ALRC, *supra* note 281, at 31.183.

[505] *See id*. at 31.192.

[506] *See* UK ICO, *supra* note 382, at 95.

[507] *See* UK ICO, *supra* note 382, at 94. 丹麥主管機關便允許向「無提供資料保護之第三國」傳遞「編碼」的訊息，因為該資訊已採取適當的保護措施，參見 Korff, *supra* note 31, at 16.

料之性質」與「對本人可能造成之傷害」後，採取技術上及組織上之必要安全維護措施。[508]

六、責任歸屬原則

「責任歸屬原則」係指：資料控制人有責任遵守相關措施，以實踐上開各項個人資料保護原則。依「個資法」之規定，公務機關或非公務機關利用敏感性個資時，應遵循之個人資料保護原則，有如下各條：

1. 第 5 條（依誠實信用方法處理個資，並尊重本人權益）；
2. 第 6 條（符合得利用敏感性個資之情形）；
3. 第 10 條（答覆本人請求）；
4. 第 11 條（確保資料正確，並更正或補充本人之敏感性個資）；
5. 第 12 條（致生損害時應通知本人）；
6. 第 16 條（公務機關利用敏感性個資，應於法定職務必要範圍內且與蒐集目的相符）或第 20 條（非公務機關利用敏感性個資，應於特定目的必要範圍內）。
7. 第 21 條（主管機關得限制非公務機關國際傳輸個人資料）

[508] 參見「個資法施行細則草案」第 9 條第 1 項。

第五節　小結

本章旨在討論公務機關或非公務機關於蒐集、處理及利用敏感性個資時，所應遵循之「個人資料保護原則」，依資料管理之流程「蒐集」、「處理」及「利用」，適用之個人資料保護原則，分述研究發現：

一、「蒐集」敏感性個資之相關個資保護原則

1. 蒐集限制原則：公務機關或非公務機關須依「個資法」第 6 條第 1 項但書規定，始能蒐集敏感性個資；公務機關或非公務機關蒐集敏感性個資，應履行告知義務，「個資法」第 8 條第 1 項與第 9 條第 1 項規定「依第 15 條或第 19 條蒐集個人資料，才需要履行告知義務」為立法疏漏，建議修正為「依本法規定」，始能將敏感性個資納入本條規範內。「個資法」第 8 條第 2 項第二款「直接蒐集之豁免告知」事由（個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要）要件與「個資法」第 6 條第 1 項但書第二款幾乎相同，如此將使公務機關或非公務機關依「個資法」第 6 條第 1 項但書第 2 款蒐集敏感性個資時，免於履行告知義務，此「豁免告知」之範圍，是否過當，仍須斟酌。本文認為，公務機關或非公務機關蒐集敏感性個資時，仍須履行告知義務，向本人告知。此外，公務機關或非公務機關嗣後變更目的，應將該資料視為未經告知程序，重新通知當事人。

2. 個人參與原則：公務機關或非公務機關違反「個資法」第 6 條第 1 項但書各款之規定，而蒐集敏感性個資者，已屬「違反本法規定」之情形，本人得依「個資法」第 11 條第 4 項，要求上開機關、機構，刪除、停止

之。此外，建議新增當事人拒絕資料管理人蒐集敏感性個資之權利：「有關第六條第一項所規定資料，當事人得請求公務機關或非公務機關，停止蒐集、處理或利用之」。

3. 資料品質原則：公務機關或非公務機關應確保敏感性個資之正確。如有違反「個資法」第 6 條「禁止蒐集、處理或利用敏感性個資料」規定時，應主動或應當事人之請求，刪除、停止蒐集、處理該敏感性個資，且應於一定期限內作成准駁之決定，並通知當事人。

4. 目的特定原則：蒐集敏感性個資之目的須明確，且符合「個資法」第 6 條第 1 項但書各款之情形。

5. 責任歸屬原則：公務機關或非公務機關「蒐集」敏感性個資時應遵循「個資法」第 5 條（依誠實信用方法蒐集個資，並尊重本人權益）；第 6 條（符合得蒐集敏感性個資之情形）；第 8 條（直接蒐集之告知義務）或第 9 條（間接蒐集告知義務）；第 10 條（答覆本人請求）；第 11 條（確保資料正確，並更正或補充本人之敏感性個資）；第 12 條（致生損害時應通知本人）；第 15 條（公務機關蒐集敏感性個資應有特定目的）或第 19 條（非公務機關蒐集敏感性個資應有特定目的）之規定

二、「處理」敏感性個資之相關個資保護原則

1. 個人參與原則：公務機關或非公務機關違反「個資法」第 6 條第 1 項但書各款之規定，而處理敏感性個資者，已屬「違反本法規定」之情形，本人得依「個資法」第 11 條第 4 項，要求上開機關、機構，刪除、停止

之。如公務機關或非公務機關之行為已對當事人造成侵害者，應查明後以適當方式通知當事人， 當事人並得請求損害賠償。

2. 資料品質原則：公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求、更正或補充之。公務機關或非公務機關如於「處理」敏感性個資時，發現疑似缺誤而欲更正或補充，此時可藉由「蒐集」敏感性個資時，已明確載明之「聯絡本人之方法」，主動聯絡本人以確認該資料之正確。

3. 目的特定原則：公務機關或非公務機關「處理」敏感性個資時，其目的仍應符合「蒐集目的之必要範圍」，亦即符合「個資法」第 6 條第 1 項但書所訂之四款要件之一。

4. 公開原則：公務機關應公開敏感性個資保有之依據（符合「個資法」第 6 條第 1 項但書列之何種例外情形）與特定目的，並避免揭露當事人之身分，至於非公務機關暫無本原則之適用。

5. 安全保障原則：建議「個資法施行細則草案」新增，公務機關或非公務機針對第六條第一項所規定之資料，採取技術上及組織上之必要措施時，應考量資料之性質與對本人可能造成之傷害。

6. 期間限制原則：公務機關或非公務機關儲存敏感性個資應符合法定列舉期限，期限屆滿時，應主動檢視該資料並立即刪除；其餘未訂定處理期間之敏感性個資，則於「特定目的」結束後，安全刪除之。

7. 責任歸屬原則：公務機關或非公務機關「處理」敏感性個資時應遵循「個資法」第 5 條（依誠實信用方法處理個資，並尊重本人權益）；第 6 條（符合得處理敏感性個資之情形）；第 10 條（答覆本人請求）；第 11 條（確保資料正確，並更正或補充本人之敏感性個資）；第 12 條（致生損害時應通知本人）；第 15 條（公務機關處理敏感性個資應有特定目的）或第 19 條（非公務機關處理敏感性個資應有特定目的）；第 17 條（公務機關應主動公開相關事項）；第 18 條（公務機關指定專人辦理安全維護措施）；第 27 條（非公務機關應採行適當安全措施）。

三、「利用」敏感性個資之相關個資保護原則

1. 個人參與原則：公務機關或非公務機關違反「個資法」第 6 條第 1 項但書各款之規定，而利用敏感性個資者，已屬「違反本法規定」之情形，本人得依「個資法」第 11 條第 4 項，要求上開機關、機構，刪除、停止之。

2. 資料品質原則：公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求、更正或補充之。

3. 目的特定原則：公務機關利用敏感性個資，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」；非公務機關利用敏感性個資，應「於蒐集之特定目的必要範圍內」為之。「個資法」第 16 條與第 20 條文字易生誤會，建議將「除第六條第一項所規定資料外」之文字予以刪除。

4. 利用之限制：公務機關或非公務機關以「原始蒐集目的以外（二次目的）」

之目的，利用敏感性個資時，應主動通知資料主體（本人）；利用敏感性個資之「二次目的」應限與原始蒐集目的有「直接相關」者，且禁止以「行銷」作為「二次目的」以利用敏感性個資料。

5. 國際傳輸：敏感性個資於進行國際傳輸時，應參考「安全保障原則」，考量「資料之性質」與「對本人可能造成之傷害」後，適度提高保護水平。

6. 責任歸屬原則：公務機關或非公務機關「利用」敏感性個資時應遵循「個資法」第 5 條（依誠實信用方法處理個資，並尊重本人權益）；第 6 條（符合得利用敏感性個資之情形）；第 10 條（答覆本人請求）；第 11 條（確保資料正確，並更正或補充本人之敏感性個資）；第 12 條（致生損害時應通知本人）；第 16 條（公務機關利用敏感性個資，應於法定職務必要範圍內且與蒐集目的相符）或第 20 條（非公務機關利用敏感性個資，應於特定目的必要範圍內）。第 21 條（主管機關得限制非公務機關國際傳輸個人資料）。

四、公務機關或非公務機關應遵守「個資法」相關規定，以落實個人資料保護原則

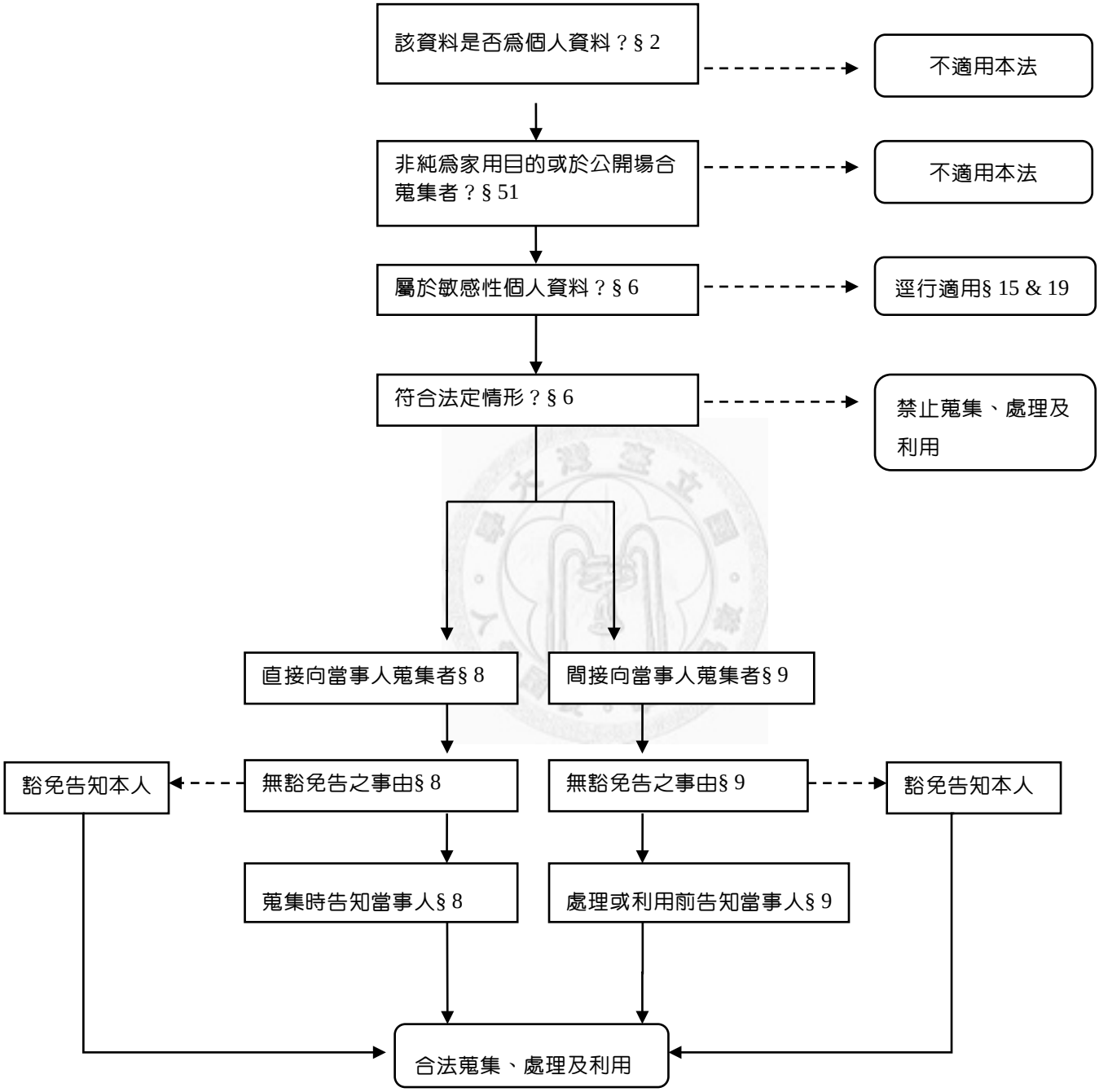
本文將公務機關或非公務機關蒐集、處理或利用敏感性個資時，應遵守之相關規定，統整列舉如后：

1. 第 5 條（依誠實信用方法蒐集、處理或利用個資，並尊重本人權益並與蒐集目的具有正當合理關連）。
2. 第 6 條（符合得蒐集、處理或利用敏感性個資之情形）。

3. 第 8 條（直接蒐集之告知義務）或第 9 條（間接蒐集告知義務）。
4. 第 10 條（答覆本人請求）。
5. 第 11 條（確保資料正確，並更正或補充本人之敏感性個資）。
6. 第 12 條（致生損害時應通知本人）。
7. 第 15 條（公務機關蒐集敏感性個資應有特定目的）或第 19 條（非公務機關蒐集敏感性個資應有特定目的）。
8. 第 16 條（公務機關利用敏感性個資，應於法定職務必要範圍內且與蒐集目的相符）或第 20 條（非公務機關利用敏感性個資，應於特定目的必要範圍內）。
9. 第 17 條（公務機關應主動公開相關事項）。
10. 第 18 條（公務機關指定專人辦理安全維護措施）或第 27 條（非公務機關應採行適當安全措施）。
11. 第 21 條（主管機關得限制非公務機關國際傳輸個人資料）。

綜上所述，茲針對公務機關或非公務機關蒐集、處理或利用敏感性個資之流程，整理如表二。

表二：公務機關或非公務機關蒐集、處理或利用敏感性個資之流程



標線說明

是

第五章　結論與建議

總結本文研究發現，茲針對我「個資法」有關敏感性個資之保護，提出下列建議。

一、「個資法」敏感性個資定義之商榷

（一）主要應考量資料之性質，並採取法律列舉方式

綜觀上開各國敏感性個資之規範方法，可知目前通說為：**法律列舉敏感性個資顯示之內容，例如醫療、基因或政治意見等個人資料，**並禁止任何人蒐集、處理或利用之。列舉說主要考量：資料之「**性質**」(nature)，認為某些性質之資料，其內容一旦揭露後，可能對個人隱私產生極大傷害，並引起社會歧視，故立法定義其為敏感性個資。

採用「法律明文列舉」之好處在於，任何人皆得迅速自行判斷該資料是否屬於敏感性個資，有助於個人資料保護之落實。其他採用「情境說」(Context-based approach)或「目的說」(Purpose-based approach)等綜合判斷模式，事涉主觀，通常須交由公正之第三人（資料主管機關或法院）才能判斷。況且，我國缺乏統一的個人資料主管機關，如將判斷敏感性個資之工作交由各類型的主管機關，敏感性個資之定義勢必形成歧異，無助於個人資料之保護，故本文建議，**有關敏感性個資之定義，仍以法律明文列舉之方式為宜**，上開「綜合判斷模式」（例如情境說）可供法院或將來有望成立之資料主管機關參考，針對部分難以避免揭露敏感性特質，作為次要輔助，以排除通念上不屬於敏感性個資之資料，例如照片或姓名等，予以豁免適用之。

（二）列舉類別待重整

「歐盟個資指令」規範五種禁止處理之敏感性個資類別，其範圍涵蓋「種族血源」、「政治意見」、「宗教或哲學信仰」、「工會會員資格」與「個人醫療與性生活」資訊，其中僅有第五種與醫療資訊有關，其他都相當程度的與「隱私」或「言論自由」有不同程度的關係。我「個資法」第 6 條列舉五種不得蒐集、處理或利用之敏感性個資，包括「醫療」、「基因」、「性生活」、「健康檢查」與「犯罪前科」，其中前四種都與「健康資訊」有關。其他有關人民表達「言論自由」（政治意見）或享有「集會結社自由」（工會會員資格）等之敏感性個資，我「個資法」則未予規範。蓋立法者或許認為我國當今「醫療資訊」遭到濫用的情形非常嚴重，基於「個人隱私」必須予以規範，惟相對於「醫療資訊」而言，有關「政治意見」與「政黨或組織會員資格」或「財務資料」，涉及憲法上「言論自由」、「集會結社自由」或「個人隱私」等權利，與個人自我表現息息相關，若不能杜絕有心人士恣意蒐集、利用這些未經公開發表，傳達「個人思想或價值觀」的資訊，藉此伺機發表，以達攻訐詆毀他人的目的，在當今的社會裡，何人得以暢所欲言，而不必害怕「秋後算帳」？是故，我國在提升「醫療資訊」保護層級的同時，對於傳達「個人思想或價值觀」之資料，例如有關表政治意見等個資，應同等保護，不得因其性質特殊，爭議過大，而乾脆不予保護，賦予有心人士或政府將手伸進我們的空間。

（三）「病歷」應併入健康相關資料

「個資法」原未將「病歷」涵蓋適用敏感性個資，本文認為係立法疏漏，建議**將「病歷」視為「醫療資料」**，並將「病歷」其自個人資料例示中刪除，以臻明確。同時，為求徹底保護資料主體（本人），且避免「醫療」或「健康檢查」適用

之疑義（不易區分且無區分實益），對於上開三種資料之定義，建議採廣義解釋，共同理解為「與個人健康相關」之資料，並**刪除「個資法」第 6 條第 1 項敏感性個資之「醫療」與「健康檢查」用語，新增為「健康」事項**。

（四）「指紋」目前無須列為敏感性個資

如前所述，資料是否為敏感性個資主要應考量該資料之「**性質**」(nature)，次要考量資料處理之情境、目的等。「指紋」屬於「生物辨識資訊」之一種，其特點在於：**完全個人化且具有與其他敏感性個資共通的特質。如遭誤用，可能導致非法之歧視，且藉由「生物辨識資訊」將可辨識出更多的個人資訊，故本文認為「指紋」應可為敏感性個資**。此外，即便「生物辨識資訊」縱然需特別處理，才能獲得資訊之內容，仍不影響該資料的性質（敏感度），因為**資料是否屬於敏感性個資與資料控制人有無能力辨識出特定個人，並無明顯的關連**。因為如果認為資料控制人須有能力自該資訊中識別出特定個人，該資訊才能作為敏感性個資，那一般人應該都無法自「醫療」或「健康檢查」資料中的血液檢測數值與「基因」資料中的基因排序資訊，獲得特定個人之資料，而使「醫療」、「健康檢查」與「基因」資料不屬敏感性個資，顯然與我「個資法」和各國實證立法規範相悖。

查前揭各國立法，並無將「生物辨識資訊」列為敏感性個資之實例，我「個資法」目前僅將「基因」（去氧核醣核酸(DNA)）列為敏感性個資，至於其他「生物辨識資訊」（例如「指紋」）則是屬於一般個資，非屬敏感性個資。本文認為，**「生物辨識資訊」之性質雖然與其他敏感性個資相似，但將「生物辨識資訊」視為敏感性個資之概念尚稱新穎，且此概念目前在國際間尚無明顯共識，故在立法者未獲得全民共識之前，本文暫不建議新增「指紋」或「生物辨識資訊」為敏感性個資**。

二、「個資法」有關得蒐集、處理或利用敏感性個資情形之例外規定之商榷

（一）現行規定有欠明確

首先，所謂「法律明文規定」應限「法律明定公務機關或非公務機關，得蒐集、處理或利用敏感性個資」者。「法律」應指「立法院三讀通過，總統公布施行之法律」。此為「個資法」須「優先適用其他法律」之情形，**限於「其他法律有特別規定（個資之蒐集、處理或利用）者」（無論寬嚴），其他法律無特別規定（個資之蒐集、處理或利用）時，仍一律適用「個資法」**。

其次，所謂「公務機關執行法定職務或私人機構履行法定義務」應限於「公務機關或非公務機關基於其法定職務或義務所必要，須蒐集、處理或利用者」。「必要」須考量其處理之目的是否合法、處理該個人資料是否為唯一達成該目的之手段、其處理與追求之目的不得顯失均衡；所謂「適當安全措施」須注意防止個人資料被竊取、竄改、毀損、滅失或洩漏，並採取技術上及組織上之必要措施。

再次，所謂「當事人自行公開」係指當事人自行對不特定人或特定多數人為揭露；所謂「其他已合法公開」則指依法規公示、公告或以其他合法方式公開之個人資料，此「合法公開」之行為應視為個人資料之「利用」，須遵守「個資法」相關規定。

最後，所謂「公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序」，其目的須限於「醫療、衛生或犯罪預防」與「統計或學術研究而有必要」，本文建議**將「統計或學術研究」用語改為「科學研究」代替**；有關「學術研究機構」之定義不明，為合理促進學術研究發展，建議**擴大定義為包括國立研究院及公私立大學研究所或其他公私立研究機構**；

有關「一定程序」之定義同樣不明，為求「個資法」用語統一且確保本款適用之個人資料無法識別特定當事人，本文建議以「經過匿名化處理，或依其揭露方式無從再識別特定本人」，代替「一定程序」之用語。

（二）應建議增列「當事人書面知情同意」及「重大公益」等例外事項

我「個資法」第 6 條第 1 項規定禁止蒐集、處理或利用敏感性個資，同條但書並規定四種得豁免禁止，而蒐集、處理或利用敏感性個資之例外情形。相較各國立法例多達八至十類，顯有不足。茲建議，參照各國立法例，增訂四類例外情形，包括「經當事人書面知情同意」、「基於預防性醫療、醫學診斷、健康照護之目的」、「為保護重大公共利益所必須」與「為保護當事人之重大利益」時，得蒐集、處理或利用敏感性個資，試修正「個資法」第 6 條第 1 項但書之條文為：

一、經當事人書面知情同意。

二、法律明文規定者。

三、公務機關執行法定職務或非公務機關履行法定義務所必要。

四、資料已經當事人自行公開或由其他已合法公開之個人資料。

五、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為科學研究而有必要，且資料須經過匿名化處理，或依其揭露方式無從再識別特定本人。

六、醫療機構基於預防性醫療、醫學診斷、健康照護之目的

七、基於重大公共利益所必要

八、為維護當事人重大利益所必要

三、敏感性個資保護不足，應予補強

（一）蒐集敏感性個資須履行告知義務

「個資法」第 8 條與第 9 條規定，公務機關或非公務機關須「依個資法第 15 條或第 19 條」蒐集個人資料時，須履行告知義務，惟「個資法」第 15 條與第 19 條卻明文排除敏感性個資之適用，將使公務機關或非公務機關蒐集或處理敏感性個資時，無須履行告知義務。此應為明顯立法疏漏，應**將第 8 條或第 9 條條文前段所謂「依第十五條或第十九條規定」用語改為「依本法規定」**，始能將敏感性個資納入本條規範內，以要求公務機關或非公務機關履行告知義務。

公務機關或非公務機關依「個資法」第 8 條第 1 項履行告知義務時，須告知本人其（公務機關或非公務機關）據以蒐集之「豁免禁止」條款（第 6 條第 1 項但書），且該條款須符合其蒐集之目的。此外，有關「個資法」第 8 條第 2 項第 2 款「直接蒐集之豁免告知」事由（個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要），其要件與「個資法」第 6 條第 1 項但書第 2 款幾乎相同，如此將使公務機關或非公務機關依「個資法」第 6 條第 1 項但書第 2 款蒐集敏感性個資時，免於履行告知義務，此「豁免告知」之範圍，是否過當，仍須斟酌，本文認為，**公務機關或非公務機關蒐集敏感性個資時，仍須履行告知義務，向本人告知**。此外，公務機關或非公務機關嗣後變更目的，應將該資料視為未經告知程序，重新通知當事人。

（二）蒐集、處理或利用敏感性個資應有特定目的，須符合「個資法」第 6 條第 1 項但書規定

「個資法」第 15 條（公務機關蒐集、處理個資應有特定目的）、第 16 條（公

務機關利用個資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）、第 19 條（非公務機關蒐集、處理個資應有特定目的）與第 20 條（非公務機關利用個資應於蒐集之特定目的必要範圍內）皆排除敏感性個資之適用。惟其用意僅在使公務機關或非公務機關得逕依第 6 條第 1 項但書之規定，以蒐集、處理敏感性個資，並非將敏感性個資排除上開條文內之「目的特定原則」外。故，公務機關或非公務機關蒐集、處理敏感性個資時，仍應有特定目的。建議將第 15 條與第 19 條所謂「除第六條第一項所規定資料外」之文字，移至同項後。第 15 條修正為：

「公務機關對個人資料之蒐集或處理，應有特定目的。**除第六條第一項所規定資料外**，應符合下列情形之一者：…」；

第 19 條修正為：

「非公務機關對個人資料之蒐集或處理，應有特定目的。**除第六條第一項所規定資料外**，應符合下列情形之一者：…」

公務機關利用敏感性個資，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」；非公務機關利用敏感性個資，應「於蒐集之特定目的必要範圍內」為之，建議修法將第 16 條與第 20 條「**除第六條第一項所規定資料外」之文字予以刪除**。

（三）敏感性個資之二次利用目的應予限縮

公務機關或非公務機關欲以「原始蒐集目的以外（二次目的）」之目的利用敏感性個資時，應適用「個資法」第 16 條或第 20 條規定，並主動通知本人（當事人）。同時，為避免過度利用敏感性個資，本文建議參考澳洲法例，將利用敏感性

個資之「二次目的」限於與原始蒐集目的有「直接相關」者，且禁止以「行銷」作為「二次目的」以利用敏感性個資料，新增「個資法」第 16 條第 2 項為：

「公務機關利用第六條第一項所規定之資料進行特定目的外之利用，其特定目的與原始蒐集目的應直接相關」；

新增第 20 條第 4 項為：

「非公務機關利用第六條第一項所規定之資料進行特定目的外之利用，其特定目的與原始蒐集目的應直接相關，且不得利用該資料行銷。

參考文獻

一、　中文文獻（依照姓名筆畫）

（一）　專書

吳庚，《行政法之理論與實用》，2005 年增訂九版，台北：自版。

財團法人資訊工業策進會科技法律研究所，《給科技研發與創新服務提供者的—個資運用藍圖》，2011 年初版，台北：商周。

葉俊榮、雷文枚、楊秀儀、牛惠之、張文貞合著，《天平上的基因—民為貴、Gene 為輕》，2006 年初版，台北：元照。

（二）　專書論文

林素鳳，〈日本個人資訊保護之法制化〉，《黃宗樂教授六秩祝賀—公法學篇（一）》，頁 107-135（2002 年 5 月），台北：新學林。

湯德宗，〈行政程序法之適用〉，《行政程序法論》，頁 133（2003 年），台北：元照。

湯德宗，〈知情同意與基因資料庫〉，《四分溪論學集：慶祝李遠哲先生七十壽辰》，頁 985-1087（2006 年），台北：允晨文化。

葉百修，〈國家賠償法〉，翁岳生主編，《行政法二〇〇〇》，頁 1357-1365（2000 年修訂二版），台北：翰蘆。

（三）　期刊

王郁琦、陳炳全，〈濫發網際網路廣告信相關法律問題之研究〉，《月旦法學》，81

期，頁 152-166（2002 年 2 月）。

余啟民，〈由肺結核病患名單資料外洩談公務機關就醫資訊管控與監督〉，《月旦民商法》，24 期，頁 8-9（2009 月 6 月）。

呂丁旺，〈淺析修正「個人資料保護法」〉，《月旦法學》，183 期，頁 131-146（2010 年 8 月）。

李建良，〈「捺指紋規定釋憲案」鑑定意見書〉，《台灣本土法學》，73 期，頁 41-44（2005 年 8 月）。

李惠宗，〈判決書上網公開與個人資訊自決權的衝突〉，《月旦法學》，154 期，頁 21-34（2008 年 3 月）

李震山、黃昭元、蔡宗珍、顏厥安，〈釋字第 603 號（全民指紋建檔案）評釋〉，《台灣本土法學》，75 期，頁 115-116（2005 年 10 月）。

周慧蓮，〈資訊隱私保護爭議之國際化〉，《月旦法學》，104 期，頁 125-126（2004 年 1 月）。

周慧蓮，〈論行動化生活之資訊隱私侵害〉，《月旦法學》，99 期，頁 152-165（2003 年 8 月）。

林秀蓮，〈個人資料保護法初探〉，《萬國法律》，頁 1（2011 年 4 月）

邱文聰，〈從資訊自決與資訊隱私的概念區分析「電腦處理個人資料保護法修正草案」的結構性問題〉，《月旦法學》，168 期，頁 172-189（2009 年 5 月）。

張冠群，〈二○○九年一月金融控股公司法關於共同行銷及關係人交易與風險集中揭露之修正條文評析〉，《月旦法學》，168 期。頁 190-215（2009 年 5 月）。

陳榮傳，〈再論資料跨國流通〉，《月旦法學》，78 期，頁 165-177（2001 年 11 月）。

楊秀儀，〈告知後同意之倫理法律再思考：縮小理論與實務的落差〉，《月旦法學》，162 期，頁 5-16（2008 年 11 月）。

廖元豪，〈高深莫測，抑或亂中有序？—論現任大法官在基本權利案件中的「審查基準」〉，《中研院法學期刊》，2 期，頁 243-244（2008 年 3 月）。

劉靜怡，〈DNA 採樣、犯罪預防和人權保障〉，《台灣法學》，124 期，頁 122（2009 年 3 月）。

劉靜怡，〈不算進步的立法：「個人資料保護法」初步評析〉，《月旦法學》，183 期，頁 153（2010 年 8 月）。

劉靜怡，〈資訊隱私權保護的國際化爭議—從個人資料保護體制的規範協調到國際貿易規範的適用〉，《月旦法學》，86 期，頁 195-205（2002 年 7 月）。

顏上詠，〈台灣人體生物資料庫管理條例草案評析〉，《月旦法學》，168 期，頁 155-171（2009 年 5 月）。

（四）學位論文

林宛怡，《以犯罪偵查為目的之 DNA 資料保存-以歐洲人權公約第八條為中心》，國立政治大學法律學研究所碩士論文（2009 年 12 月）。

曾珮瑩，《全民指紋建檔爭議之研究-以 94 年換證為例》，銘傳大學公共事務學系碩士論文（2008 年）。

熊愛卿，《網際網路個人資料保護之研究》，國立台灣大學法律研究所博士論文，（1999 年）。

（五）會議論文

湯德宗，〈電腦處理個人資料保護法 2008 修正草案評釋〉，發表於台灣法學會 2008 年年度法學會議（2008 年 12 月 20 日）

（六） 政府公報

立法院公報，99 卷 26 期，頁 67（2010 年 4 月）。

立法院公報，99 卷 29 期，頁 376（2010 年 5 月）。

監察院公報，2196 卷，頁 301-306（1999 年 2 月 10 日）

監察院公報，2232 卷，頁 2299-2307（1999 年 10 月 20 日）

監察院公報，2310 卷，頁 76-77（2001 年 04 月 18 日）

監察院公報，2312 卷，頁 1-6（2001 年 05 月 02 日）

監察院公報，2316 卷，頁 54-55（2001 年 05 月 30 日）

監察院公報，2317 卷，頁 11-19（2001 年 06 月 06 日）

二、　外文文獻

（一）　專書

Allen, Anita L. & Richard C. Turkington (2002), Privacy Law: Cases and Materials, MN: West Group.

Australian Law Reform Commission (2008), For Your Information: Australian Privacy Law and Practice, Vol. 1-3, available at http://www.alrc.gov.au/publications/report-108

Bainbridge, David (1996), EC Data Protection Directive, London: Butterworths.

Carey Peter (2004), Data Protection: A Practical Guide to UK and EU Law, N.Y.: Oxford Univ. Press.

Coppel, Philip (2007), Information Rights, London: Sweet & Maxwell.

Hill, David G. (2009), Data Protection: Governance, Risk Management, and Compliance, MA: CRC Press.

Jay, Rosemary & Angus Hamilton(2003), Data Protection: Law And Practice

Kuner, Christopher (2007), European Data Protection Law: Corporate Compliance and

Regulation, N.Y.: Oxford Univ. Press.

Macdonald QC, John & Clive H. Jones eds. (2003), The Law of Freedom of Information, N.Y.: Oxford Univ. Press.

Mills, Jon L. (2008), Privacy: The Lost Right, N.Y.: Oxford Univ. Press.

Morgan, Richard & Ruth Boardman (2003), Data Protection Strategy: Implementing Data Protection Compliance, London: Sweet & Maxwell.

Singleton, Susan & Lynda A. C. Macdonald & Norman Green (2004), Data Protection: A Guide to Legal Compliance for HR And Payroll, UK: Tottel Publishing.

（二） 專書論文

Beckman, Christel (2011), Regulating Privacy: Vocabularies of Motive in Legislating Right of Access to Criminal Records in Sweden, in Serge Gutwirth, Yves Poullet, Paul De Hert, Ronald Leenes eds., Computers, Privacy and Data Protection: an Element of Choice 111-37.

Beyleveld, Deryck & Andrew Grubb et al. (2004), The UK Implementation of Directive 95/46/EC, in Deryck Beyleveld et al. eds., Implementation of the Data Protection Directive in Relation to Medical Research in Europe.

Beyleveld, Deryck (2004), The Duty to Provide Information to the Data Subject: Articles 10 and 11 of directive 95/46/EC, in Deryck Beyleveld et al. eds., The Data Protection Directive and Medical Research Across Europe 69-87.

Brownsword, Roger (2009), Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality, in Serge Gutwirth, Yves Poullet, Paul De Hert, C´ecile de Terwangne & Sjaak Nouwt eds., Reinventing Data Protection? 83-109.

Bygrave, Lee A. (2002), Core Principles of Data Protection Laws, in Data Protection

Law: Approaching Its Rationale, Logic and Limits 344.

Casabona, Carlos María Romeo (2004), Anonymization and Pseudonymization: The Legal Framework at a European Level, in Deryck Beyleveld, David Townend, Ségolène Rouillé-Mirza & Jessica Wright eds., The Data Protection Directive and Medical Research Across Europe 33-49.

Deryck Beyleveld & Andrew Grubb et al. (2004), The UK Implementation of Directive 95/46/EC, in Deryck Beyleveld, David Townend, Ségolène Rouillé-Mirza & Jessica Wright eds., Implementation of the Data Protection Directive in Relation to Medical Research in Europe 417.

Dhillon, Gurpreet & Ella Kolkowska (2010), Can a Cloud Be Really Secure? A Socratic Dialogue, in Serge Gutwirth, Yves Poullet, Paul De Hert & Ronald Leenes eds., Computers, Privacy and Data Protection: an Element of Choice 348.

Lehtonen, Lasse A. (2004), Genetic Information and the Data Protection Directive of the European Union, in Deryck Beyleveld, David Townend, Ségolène Rouillé-Mirza & Jessica Wright et al. eds., The Data Protection Directive and Medical Research Across Europe 103-112.

Nys, Herman (2004), The Scope of Exemptions for Medical Research, in Deryck Beyleveld, David Townend, Ségolène Rouillé-Mirza & Jessica Wright et al. eds., The Data Protection Directive and Medical Research Across Europe 53.

Ofner, Helmut (2004), Data Protection in Austria, in Deryck Beyleveld, David Townend, Ségolène Rouillé-Mirza & Jessica Wright et al. eds., Implementation of the Data Protection Directive in Relation to Medical Research in Europe 13.

Prudil, Lukáš & Josef Kuře (2005), Research Ethics Committees in the Czech Republic, in Deryck Beyleveld, David Townend & Jessica Wright et al. eds., Research Ethics Committees, Data Protection and Medical Research in European Countries 31-39.

Purtova, Nadezhda (2011), Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence, in Serge Gutwirth, Yves Poullet, Paul De Hert & Ronald Leenes eds., Computers, Privacy and Data Protection: an Element of Choice 39-64.

Rosenzweig, Mary & Lisbeth Kundsen (2005), Research Ethics Committees in Denmark, in Deryck Beyleveld, David Townend & Jessica Wright et al. eds., Research Ethics Committees, Data Protection and Medical Research in European Countries 37.

Rouillé-Mirza Ségolène & Jessica Wright (2004), Comparative Study on the Implementation and Effect of Directive 95/46/EC on Data Protection in Europe: Medical Research, in Deryck Beyleveld, David Townend, Ségolène Rouillé-Mirza & Jessica Wright et al. eds., The Data Protection Directive and Medical Research Across Europe 189-230.

Rouillé-Mirza, Ségolène & Jessica Wright (2004), Comparative Study on the Implementation and Effect of Directive 95/46/EC on Data Protection in Europe: General Standards, in Deryck Beyleveld, David Townend, Ségolène Rouillé-Mirza & Jessica Wright eds., The Data Protection Directive and Medical Research Across Europe 125-87.

Rouvroy, Antoinette & Yves Poullet (2009), The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, in Serge Gutwirth, Yves Poullet, Paul De Hert, C´ecile de Terwangne & Sjaak Nouwt eds., Reinventing Data Protection? 68.

Townend, David (2004), Overriding Data Subjects' Rights in the Public Interest, in Deryck Beyleveld et al. eds., The Data Protection Directive and Medical Research Across Europe 97.

（三） 期刊

Adams, Carlisle (2006), A Classification for Privacy Techniques, 3(1) U. Ottawa L. & Tech. J. 35.

Burke Michael E. (2005), Demetrios Eleftheriou, Marco Berliri & Giulio Coraggio, Infonnation Services, Technology, and Data Protection, 39 Int'l Law. 403, 408-409.

Bygrave, Lee A. (1998), Data Protection Reform in Scandinavia, 5 Privacy L. & Pol'y Rep. 9-12.

Bygrave, Lee A. (2001), The Place of Privacy In Data Protection Law, 24 U.N.S.W.L.J. 277, 280.

Callens, Stefaan (1995), The Privacy Directive and Use of Medical Data for Research Purposes, 2 Euro. J. Health L. 309.

Evans, A. C. (1981), European Data Protection Law, 29 Am. J. Comp. L. 571.

Farnsworth, David P. (1983), Data Privacy or Data Protection and Transborder or Transnational Data Flow, an American's View of European Legislation, 11(4) Int'L Bus. Law. 114.

Greenleaf, Graham (2005), APEC's Privacy Framework: A new low standard, 11(5) Privacy L. & Pol'Y Rep. 121-125.

Greenleaf, Graham (2009), Five years of the APEC Privacy Framework: Failure or promise?, 25 Computer L. & Security Rev. 28.

Greenleaf, Graham (2012), Global Data Privacy Laws: 89 Countries, and Accelerating, 115 Privacy L. & Bus. Int'l Rep. 1.

Hondius, Frits W. (1980).Data Law in Europe, 16 Stan. J. Int'l L. 87.

McCullagh, Karen (2007), Data Sensitivity: Proposals for Resolving the Conundrum, 2

J. Int’L Com. L. & Tech. 190.

Mei, Peter (1993), The EC Proposed Data Protection Law, 25 L. & Pol’Y Int’L Bus. 305.

Miller, Maeve Z. (2007), Note, Why Europe Is Safe from Choicepoint: Preventing Commercialized Identity Theft through Strong Data Protection and Privacy Laws, 39 Geo. Wash. Int’L L. Rev. 395-421.

Oliveira, Julia de (2011), EU Directive and CoE Convention are being revised in parallel, 109 Privacy L. & Bus. Int’L Rep. 23.

Rosenbaum, Joseph I. (1992-1993), The European Commission’s Draft Directive on Data Protection, 33 Jurimetrics J. 1.

Schwartz, Paul M. (1994-1995), European Data Protection Law and Restrictions on International Data Flows, 80 Iowa L. Rev. 471.

Shaffer, Gregory (2000), Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25 Yale J. Int'l L. 1, 30.

Stadlen, Godfrey (1976), Survey of National Data Protection Legislation, 3(3) Computer Networks 174-186.

Tapper, Colin (1992), New European Direction in Data Protection, 3(1) J.L. & Info. Sci. 9.

Turn, Rein (1976), Classif ication of Personal Information for Privacy, National Computer Conference and Exposition 303-304.

Wong, Rebecca (2007), Date Protection Online: Alternative Approaches to Sensitive Data, 2(1) J. Int’L Com. L. & Tech. 9.

（四） 研究報告

California Office of Information Security and Privacy Protection , Recommended Practices for Protecting the Confidentiality of Social Security Numbers, available at http://www.privacy.ca.gov/res/docs/pdf/ssnrecommendations.pdf

Canadian Institutes of Health Research, Questions And Answers For Health Researchers, available at http://publications.gc.ca/collections/Collection/MR21-25-2001E.pdf

Comparative Study of European Commission Directorate-General Justice (2010), Freedom And Security on Different Approaches to New Privacy Challenges, In Particular in the Light of Technological Developments- B.1 – United States Of America, May. 2010, available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf

Comparative Study of European Commission Directorate-General Justice, Freedom And Security on Different Approaches to New Privacy Challenges, In Particular in the Light of Technological Developments- B.2 –Australian, at 18 (May. 2010) available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B2_australia.pdf

Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data para.1, available at https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=564487&SecMode=1&DocId=560582&Usage=2

Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data Principle

Financial Services Agency, Guidelines for Personal Information Protection in the Financial Field Art. 6, available at http://www.fsa.go.jp/frtc/kenkyu/event/20070424_02.pdf

Gassmann, Hans Peter (2010), Former Head of the ICCP Division Directorate for Science, Technology and Industrtry, OECD 30 Years After: The Impact of The OECD Privacy Guidelines, Address at Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and its Working Party on Information Security and Privacy (WPISP) (Mar. 10, 2010), http://www.oecd.org/document/39/0,3746,en_2649_34255_44946983_1_1_1_1,00.html

Graux,Neil Robinson Hans, Maarten Botterman & Lorenzo Valeri (2009), Technical Report, Review of the European Data Protection Directive, UK: ICO, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf

Korff, Douwe (2002), EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws 14 (Sep. 2002), available at http://www.garanteprivacy.it/garante/document?ID=455584

Kruse, Andreas, Camino Mortera-Martinez, Véronique Corduant & Sebastian Lange (2008), Final Report, The Regulatory Framework for RFID, at 13 (Aug. 2008), available at www.rfid-in-action.eu/public/results/legal-aspects/framework.pdf

Ministry of Economy, Trade and Industry, Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information 36 (2009), available at http://www.meti.go.jp/policy/it_policy/privacy/0910english.pdf

Rodrigues et al., Roberto J. (2001), The Regulation of Privacy and Data Protection in The Use of Electronic Health Information 76.

Simitis, Spiros (1999), Revisiting Sensitive Data, 1 Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, available at http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Simitis_1999.pdf

Study Report of the European Commission against Racism and Intolerance on“Ethnic” statistics and data protection in the Council of Europe countries, at 24 (Oct. 10, 2007), available at http://www.coe.int/t/dghl/monitoring/ecri/activities/themes/Ethnic_statistics_and_data_protection.pdf

UK ICO, The Guide to Data Protection, available at http://www.ico.gov.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/THE_GUIDE_TO_DATA_PROTECTION.ashx

UK Information Commissioner, DPA: Legal Guidance, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

（五）案例

M.S v. Sweden [1997] 28 EHRR 313, para 34-35

Nat'l Sec. News Serv. v. U.S. Dep't of Navy, 584 F. Supp. 2d 94, 96 (D.D.C. 2008)

Stone v. South East Coast Strategic Health Authority [2006] EWHC 1668 (Admin) [2007] (Eng.)