

行政機關資料蒐集與個資保護

世新大學法律學院副教授 謝碩駿

要 目

壹、緒說

貳、行政機關蒐集個人資料作為基本權干預措施

一、受干預之基本權

(一) 資訊隱私權

(二) 秘密通訊自由

二、資訊隱私權保障範圍內之資料：個人資料

(一) 個人資料之意義

(二) 個人資料之去識別化處理

參、行政機關蒐集個人資料之合法性要求

一、須具有特定蒐集目的

二、經當事人同意

三、對當事人權益無侵害

四、執行法定職務

五、必要性

六、尊重當事人之權益

肆、台北市政府單一識別系統之問題

一、法律依據？

二、當事人經明確告知而同意？

(一)告知義務之豁免？

(二)告知內容之明確性？

1.蒐集機關？

2.蒐集之目的？

3.蒐集之資料類別？

三、必要性？

壹、緒說

行政機關為了履行各種行政任務並作成各種行政決定，須以一定之資訊為據，從而有蒐集資料之需求。行政程序法第 36 條也規定：「行政機關應依職權調查證據」，明文揭櫫職權調查原則，彰顯行政機關所為之資料蒐集活動在行政程序中的重要性。行政機關蒐集的資料中，有許多具有個人資料之性質，在司法院釋字第 603 號解釋肯認憲法保障人民對個人資料擁有自主決定地位後，行政機關所為之個人資料蒐集行為，是否符合個人資料保護法規定之各項合法性要求，已逐漸成為當代公法學的熱門議題。近來，台北市政府訂定發布「台北市政府單一識別服務作業要點」，據以蒐集人民之個人資料作為單一識別資料，並建置單一識別系統整合各項身分辨識作業，其能否通過個人資料保護法各項合法要件之檢驗，更是備受關注。行政機關所為之個人資料蒐集行為，無論在行政程序上具有如何之重要意義，終究不得逾越個人資料保護之合法界線，有鑑於此，本文擬以「行政機關資料蒐集與個資保護」為題，針對與此相關之各項合法性要求，一一予以探究釐清。首先，本文將先從憲法的層次出發，說明行政機關所為之個人資料蒐集措施，在憲法上（尤其對基本權保障而言）之意義¹。其次，本文將以個人資料保護法之規定為依據，分析行政機關蒐集個人資料應符合之合法性要求²。接著，本文將以各項合法性要求作為標準，檢視台北市政府單一識別系統在法律上之疑義³，最後並出總結⁴。在展開正式討論前，要先說明的是，歐盟在 2016 年 4 月通過「個人資料保護基本規章」（General Data Protection Regulation, GDPR），取代原本的歐盟「個人資料保護指令」（Data Protection Directive, Directive

¹ 請參見本文「貳」。

² 請參見本文「參」。

³ 請參見本文「肆」。

⁴ 請參見本文「伍」。

95/46/EC)，並自 2018 年 5 月 25 日生效施行，成為可在歐盟各成員國內直接適用之法規範，無須轉換為歐盟各成員國之國內法。依據歐盟個人資料保護基本規章第五章「個人資料傳輸至第三國或國際組織」（第 44 條至第 50 條）之規定，原則上，歐盟境內之個人資料禁止跨境傳輸至第三國或國際組織，除非符合一定之例外容許要件。「歐盟境內個人資料跨境對外傳輸」的例外容許要件之一，乃是依歐盟個人資料保護基本規章第 45 條規定「通過歐盟執行委員會的適足性認定」，質言之，該第三國或國際組織對於個人資料保護，必須被歐盟執行委員會認定具有「適當之水準」，而所謂「適當之水準」，則是指「與歐盟同等之保障水準」⁵。由於行政院國家發展委員會（主任委員）已向歐盟表達我國有意願申請取得個人資料保護之適足性認定⁶，所以為了通過歐盟的適足性認定，歐盟個人資料保護基本規章對我國而言，已非事不關己的異國法規，我國必須努力將個人資料保護法制調整成和歐盟個人資料保護基本規章具有同等的保障水準。在這樣的背景下，本文在討論各該問題時，會一併以歐盟個人資料保護基本規章作為比較觀察的對象。

貳、行政機關蒐集個人資料作為基本權干預措施

一、受干預之基本權

（一）資訊隱私權

大法官在 2005 年 9 月 28 日針對戶籍法第 8 條之違憲疑義⁷，作成司法院釋

⁵ Christoph Klug, in: Peter Gola (Hrsg.), Datenschutz-Grundverordnung Kommentar, 2. Aufl., 2018, Art. 45 Rn. 5.

⁶ 中央通訊社，因應 GDPR 陳美伶訪歐盟表達盼取得適足性認定，2018 年 6 月 1 日，<https://www.cna.com.tw/news/aopl/201806010116.aspx>（最後瀏覽日：2019 年 11 月 3 日）。

⁷ 2005 年施行之戶籍法，係以 1997 年 5 月 21 日總統公布的版本為基礎（現行之戶籍法則是以 2008 年 5 月 28 日總統公布之版本為基礎），該版本戶籍法第 8 條規定：「（第 1 項）人民年滿十四歲者，應請領國民身分證；未滿十四歲者，得申請發給。（第 2 項）依前項請領國民身分證，

字第 603 號解釋，宣告戶籍法第 8 條強制人民按捺指紋並錄存之規定，對人民的資訊隱私權造成不符比例原則之限制，具有違憲性並立即失效。本號解釋最值得注意之處，乃是大法官以憲法第 22 條為依據，導出「資訊隱私權」此一憲法未明文列舉之基本權。關於資訊隱私權之保障內涵，本號解釋指出：「維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障（本院釋字第五八五號解釋參照）。其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權」。

大法官在司法院釋字第 603 號解釋中，首先（援引司法院釋字第 585 號解釋為先例）以人性尊嚴與人格權之保障為基礎，認為隱私權乃是「不可或缺」的基本權，在憲法未明文列舉保障的情況下，應受憲法第 22 條（基本權概括保障條款）保障。以「隱私權應受憲法第 22 條保障」為前提，大法官接著聚焦在「資訊隱私」的面向，認為隱私權的保障範圍包括對於資訊隱私之保障，並因此推導出「資訊隱私權」的概念。觀察司法院釋字第 603 號解釋對於資訊隱私權的闡述，可以得知，此一憲法未明文列舉的基本權，其保障內涵分成三個部分：（一）揭露個人資料之決定權、（二）使用個人資料之知悉與控制權、（三）個人資料記載錯誤之更正權。由這三個保障內涵共同型塑而成的資訊隱私權，大法官認為其保

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」。依本條第 2 項及第 3 項之規定，人民被強制必須捺指紋並錄存，否則將承受無法請領國民身分證的不利後果。立法委員賴清德等八十五人認為 1997 年版本之戶籍法第 8 條第 2 項及第 3 項有違憲疑義，遂依司法院大法官審理案件法第 5 條第 1 項第 3 款之規定，向大法官聲請釋憲。

障核心要旨就在於「個人自主控制個人資料」⁸。

從比較法的角度來看，大法官透過司法院釋字第 603 號解釋（並以憲法第 22 條為依據）推導出的資訊隱私權，其實和德國聯邦憲法法院發展出的「資訊自主決定權」（*Recht auf informationelle Selbstbestimmung*）雷同度甚高⁹。德國聯邦憲法法院在 1983 年「人口普查案」判決（*Volkszählungsurteil*）¹⁰中，以德國基本法第 2 條第 1 項（一般人格權之保障）結合德國基本法第 1 條第 1 項（人性尊嚴之保障）為依據，發展出德國基本法未明文列舉的資訊自主決定權。依照德國聯邦憲法法院的闡述，資訊自主決定權的保障內涵，乃在保障每個人享有「原則上得自主決定其個人資料之揭露與使用」的權能¹¹。質言之，作為資訊自主決定權的權利主體，每個人均有權自主決定其個人資料是否、何時、對誰、如何揭露¹²。從德國聯邦憲法法院對資訊自主決定權的定名以及保障內涵的闡述，不難得知，資訊自主決定權要保障的客體，既非「個人資料本身」，也非「個人資料內容的私密性」，而是「每個人在完整的人格下，對其個人資料之自主決定地位」。在涉及資訊自主決定權的諸多裁判中，德國聯邦憲法法院就清楚指出，對於資訊自主決定權的保障而言，個人資料的內容是否具有私密敏感性，其實並不重要，即便是公開可得的個人資料，也同樣受資訊自主決定權保障¹³。

⁸ 司法院釋字第 603 號解釋：「其中就個人自主控制個人資料之資訊隱私權而言，...」。

⁹ 相同看法：詹鎮榮，公務機關間個人資料之傳遞－以臺灣桃園地方法院行政訴訟 102 年度簡字第 2 號判決出發，載於：法學叢刊，第 60 卷第 1 期，2015 年 1 月，頁 7-8。

¹⁰ BVerfGE 65, 1 ff.

¹¹ BVerfGE 65, 1 (43). 此乃德國聯邦憲法法院自「人口普查案」判決以來，迄今未曾改變的看法，參見：BVerfGE 113, 29 (46); 115, 166 (188).

¹² *Horst Dreier*, in: *Horst Dreier* (Hrsg.), *Grundgesetz Kommentar*, Bd. 1, 3. Aufl., 2013, Art. 2 I Rn. 79; *Friedhelm Hufen*, *Staatsrecht II Grundrechte*, 7. Aufl., 2018, § 12 Rn. 4; *Hans D. Jarass*, in: *Hans D. Jarass/Bodo Pieroth*, *Grundgesetz für die Bundesrepublik Deutschland Kommentar*, 15. Aufl., 2018, Art. 2 Rn. 42; *Dietrich Murswiek/Stephan Rixen*, in: *Michael Sachs* (Hrsg.), *Grundgesetz Kommentar*, 8. Aufl., 2018, Art. 2 Rn. 73.

¹³ BVerfGE 118, 168 (185); 120, 378 (398 f.); *BVerfG*, Beschluss des Ersten Senats vom 18. Dezember 2018, - 1 BvR 142/15 -, Rn. 38 f., http://www.bverfg.de/e/rs20181218_1bvr014215.html (letzter

大法官在司法院釋字第 603 號解釋透過憲法第 22 條導出的基本權，雖然定名為資訊隱私權，但從保障要旨（個人自主控制個人資料）觀之，其實無關乎隱私（資料的私密性），而是如同德國聯邦憲法法院發展出的資訊自主決定權一樣，以「每個人對其個人資料享有自主決定地位」作為保障客體。也正因如此，所以司法院釋字第 603 號解釋將憲法對於「個人自主控制資料」的基本權保障稱為「資訊隱私權」，嚴格說來，其實並未精確表達出此一基本權真正的保障內涵，甚至可能會引起誤解，讓人誤以為此一基本權只涉及「具隱私性的資料」。

（二）秘密通訊自由

憲法第 12 條保障之秘密通訊自由，係對人民「通訊過程」隱密性之保障¹⁴，因此乃是一種保障時間有限制的基本權，其保障時點始於通訊開始，終於通訊結束¹⁵。大法官在司法院釋字第 631 號解釋（理由書）以及第 756 號解釋（理由書）闡述憲法第 12 條保障的秘密通訊自由時，明確指出，憲法第 12 條「旨在確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利。此項秘密通訊自由乃憲法保障隱私權之具體態樣之一，為維護人性尊嚴、個人主體性及人格發展之完整，並係保障個人生活私密領域免於國家、他人任意侵擾及維護個人資料之自主控制，所不可或缺之基本權利」。在這兩號司法院解釋的肯認下，個人資料之自主控制，除了受資訊隱私權（憲法第 22 條）保障，同時也在憲法第 12 條的保障範圍內。從憲法第 22 條導出的資訊隱私權，對個人

Zugriff am 5.11.2019).

¹⁴ 東吳公法中心憲法小組主編，憲法講義，2018 年 3 月，頁 280（范秀羽執筆）；陳新民，憲法學釋論，9 版，2018 年 7 月，頁 216。

¹⁵ 吳信華，憲法釋論，3 版，2018 年 9 月，邊碼 676。德國法上對於通訊秘密保障（德國基本法第 10 條）的同樣理解，參見：BVerfGE 115, 166 (186); *Christoph Gusy*, in: Peter M. Huber/Andreas Voßkuhle (Hrsg.), Grundgesetz Kommentar, Bd. 1, 7. Aufl., 2018, Art. 10 Rn. 44; *Georg Hermes*, in: Horst Dreier (Hrsg.), Grundgesetz Kommentar, Bd. 1, 3. Aufl., 2013, Art. 10 Rn. 38; *Hufen* (Fn. 12), § 17 Rn. 5; *Jarass* (Fn. 12), Art. 10 Rn. 7; *Ralf P. Schenke*, in: Klaus Stern/Florian Becker (Hrsg.), Grundrechte-Kommentar, 3. Aufl., 2019, Art. 10 Rn. 48.

資料之自主決定提供了一般性的保障；而憲法第 12 條的秘密通訊自由，則基於保障時間之限制，成為人民在通訊活動過程中，用來防禦國家蒐集、處理、利用個人資料的依據。資訊隱私權以及秘密通訊自由都對個人資料之自主決定提供了憲法層次的保障，而秘密通訊自由的保障則僅侷限在通訊活動過程中，因此對於個人資料之自主決定而言，資訊隱私權乃是普通保障規定，秘密通訊自由則是特別保障規定，二者具有普通法與特別法的關係¹⁶。國家侵入人民進行之通訊活動蒐集個人資料，無論後續在處理或利用該個人資料時，人民的通訊活動是否已經結束，均構成對秘密通訊自由之干預¹⁷。至於在通訊活動結束後，國家蒐集因為該通訊活動而產生之個人資料，就個人資料之自主決定而言，則已不在秘密通訊自由的保障範圍內，而由資訊隱私權以普通保障規定的地位予以承接保障¹⁸。

二、資訊隱私權保障範圍內之資料：個人資料

（一）個人資料之意義

行政機關的資料蒐集行為，涉及的資料種類非常多，只有在被蒐集的資料具有個人資料的性質時，才會觸及憲法對個人資料自主決定地位的基本權保障¹⁹。大法官在司法院釋字第 585 號解釋（理由書）、第 603 號解釋、第 631 號解釋（理由書）以及第 756 號解釋（理由書）提到「個人資料之自主控制」時，並未進一步說明何謂個人資料。就現行法而言，目前唯一對個人資料這個概念設有明確立

¹⁶ BVerfGE 100, 313 (358); *Gusy* (Fn. 15), Art. 10 Rn. 43; *Hermes* (Fn. 15), Art. 10 Rn. 103; *Hufen* (Fn. 12), § 17 Rn. 10; *Jarass* (Fn. 12), Art. 2 Rn. 38; *Martin Pagenkopf*, in: Michael Sachs (Hrsg.), *Grundgesetz Kommentar*, 8. Aufl., 2018, Art. 10 Rn. 53; *Schenke* (Fn. 15), Art. 10 Rn. 114.

¹⁷ BVerfGE 115, 166 (186 f.); *Schenke* (Fn. 15), Art. 10 Rn. 114.

¹⁸ BVerfGE 115, 166 (187); *Gusy* (Fn. 15), Art. 10 Rn. 44; *Hufen* (Fn. 12), § 17 Rn. 10; *Schenke* (Fn. 15), Art. 10 Rn. 114.

¹⁹ 行政機關蒐集之資料不具有個人資料的性質，並不代表因此就不涉及基本權利之干預，因為與個人資料無關的資料蒐集措施（例如行政機關蒐集的是公司營業資料），仍可能對憲法第 15 條財產權等其他基本權構成干預效果。

法定義的，乃是個人資料保護法第 2 條第 1 款。至於其他法規，則均直接將個人資料此一概念當成構成要件要素使用，並指示連結到個人資料保護法的規定²⁰。既然憲法本身與大法官歷來所作涉及「個人資料自主控制」的解釋，沒有對個人資料予以定義，而現行各法規對於個人資料此一概念之使用，也未見有與個人資料保護法相異之規定，那麼要探究行政機關的資料蒐集行為是否已觸及憲法對個人資料自主決定地位之保障，在認定被行政機關蒐集的資料是否屬於個人資料時，也就應該以個人資料保護法第 2 條第 1 款的立法定義為準。

依據個人資料保護法第 2 條第 1 款之定義，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」。另外，個人資料保護法施行細則第 2 條規定：「本法所稱個人，指現生存之自然人」。在個人資料保護法第 2 條第 1 款以及個人資料保護法施行細則第 2 條的定義下，個人資料以「現生存之自然人」的資料為限，法人的資料從而被排除在個人資料的範圍外²¹。在個人資料保護法第 2 條第 1 款中，立法者首先以明文例示的方式，將姓名、出生年月日等資料直接劃入個人資料的概念範疇內，而未在例示清單內的資料，如果是「得以直接或間接方式識別個人」之資料，即具有個人資料之性質。「得以直接方式識別個人」之資料，是指直接依據該資料便能連結到特定個人並從而識別出特定個人²²，最常見的當然就是特定個人的姓名²³。至於「得以間接方式識別

²⁰ 例如無人載具科技創新實驗條例第 17 條規定：「申請人蒐集、處理或利用個人資料，應遵守個人資料保護法之相關規定」。又例如公有及接受補助文化資產資料公開辦法第 10 條規定：「本辦法規定涉及著作權、個人資料者，應依著作權法、個人資料保護法或相關法令規定辦理」。

²¹ 由於大法官在司法院釋字第 603 號解釋中，是從憲法第 22 條對於人格權的保障推導出資訊隱私權（個人資料自主決定權），所以個人資料保護法第 2 條第 1 款將個人資料概念的指涉範圍侷限在自然人的資料，而排除法人的資料，倒也與「資訊隱私權乃人格權保障之具體樣態」相契合。

²² 范姜真嫩，個人資料保護法關於「個人資料」保護範圍之檢討，載於：東海大學法學研究，第 41 期，2013 年 12 月，頁 97-98。

個人」之資料，依據個人資料保護法施行細則第 3 條之規定，則是指「保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人」。雖然「間接識別能力」之判斷，應該要以「社會一般多數人得間接識別」抑或「任何人得間接識別」為基準，在學說上仍有爭議²⁴，但至少可以確定的是，個人資料的認定已不再侷限於是否指名道姓「直接識別」特定個人，某一筆資料若在與其他資料相互比對後能識別出特定個人，該資料即是個人資料²⁵。在行政實務上，常見誤以為「某一筆資料沒有指名道姓，不能從該資料直接識別特定個人，該資料即非個人資料」的想法，乃是對個人資料採取過於狹隘的理解²⁶，不但不符合個人資料保護法對於個人資料的定義，也

²³ 劉定基，個人資料的定義、保護原則與個人資料保護法適用的例外－以監視錄影為例（上），載於：月旦法學教室，第 115 期，2012 年 5 月，頁 48。

²⁴ 認為應以「社會一般多數人得間接識別」為判斷基準者：范姜真嫻，前註 22，頁 98-99。認為應以「任何人得間接識別」為判斷基準者：張陳弘，個人資料之認定－個人資料保護法適用之啟動閥，載於：法令月刊，第 67 卷第 5 期，2016 年 5 月，頁 97。

²⁵ 例如記名悠遊卡之卡號，由於能透過資料庫之比對，得知該卡號背後的特定個人，因此（至少對於悠遊卡公司而言）屬於個人資料。參見：2011 年 5 月 13 日法務部法律字第 0999051927 號函。

²⁶ 舉個簡單的例子：台北市政府要在各級學校內設置智慧販賣機，鼓勵學生透過結合悠遊卡功能的數位學生證以電子支付方式消費，此一措施引起社會上對於個人資料保護之疑慮。對於此等疑慮，台北市政府教育局在 2019 年 10 月 7 日發布的新聞稿指出：「機臺系統只能讀取卡號，廠商無法存取個資，請各界放心」（新聞稿全文載於：https://www.doe.gov.taipei/News_Content.aspx?n=B8E0D00523CEF081&s=E575D1AD7E7C2A45，最後瀏覽日：2019 年 11 月 10 日）。很明顯地，台北市政府教育局認為，被校園智慧販賣機讀取的悠遊卡卡號，並不是個資。同樣的想法也出現在悠遊卡公司董事翟本喬先生的個人意見，其認為只有把悠遊卡卡號、學號以及學生「真正的個人資料」相串連，才能把學生在智慧販賣機的消費內容連結到個人資料（參見：自由時報，台北市推智慧販賣機恐洩漏個資？翟本喬反駁，2019 年 10 月 8 日，<https://news.ltn.com.tw/news/politics/breakingnews/2939616>，最後瀏覽日：2019 年 11 月 10 日）。上述的想法，顯然都不符合個人資料保護法第 2 條第 1 款對於個人資料的定義。與學生證相結合的悠遊卡，其卡號在與學生證學號以及學生學籍資料相互比對後，即能透過該悠遊卡卡號識別出特定個人（也就是持卡的學生是誰），所以並非只有學校才擁有學生「真正的個人資料」，那些因為學生以電子支付方式消費而被智慧販賣機廠商讀取的學生悠遊卡卡號，本身

忽略了對該資料之蒐集、處理與利用構成資訊隱私權干預的嚴肅憲法意義。

(二) 個人資料之去識別化處理

在個人資料保護法第 2 條第 1 款的定義下，個人資料乃是得以直接或間接方式識別特定個人之資料。既然個人資料是得識別特定個人的資料，那麼一旦將個人資料作了去識別化處理之後，該資料是否還具有個人資料的性質呢？對於這個問題，法務部 2014 年 11 月 4 日法律字第 10303510410 號函指出：「如交通管理機關將 ETC 資料以代碼、匿名、隱藏部分資料或其他使他人無從辨識該特定個人方式，進行去識別化處理後，已無從識別特定當事人，即無個人資料保護法適用」；另外，法務部 2014 年 11 月 17 日法律字第 10303513040 號函也同樣認為：「如將公務機關保有的個人資料運用技術去識別化而呈現方式已無從直接或間接識別特定個人，即非屬個人資料」。從法務部上開兩號函釋的見解加以延伸，由於個人資料經去識別化處理後已不具有個人資料的性質，所以如果行政機關蒐集的資料是「經去識別化處理後的個人資料」，即非個人資料蒐集措施，從而並不構成資訊隱私權之干預。

法務部在上開兩號函釋主張「個人資料經去識別化處理後，已非個人資料，故無個人資料保護法之適用」，就本文看來，單純就論理邏輯而言，此等見解可以贊同。然而，如果拿歐盟的標準來相比，在我國個人資料保護法中規定的「去識別化處理」，其實離真正的去識別化還有一大段差距，以致於在我國個人資料保護法的標準下對個人資料進行去識別化處理，是否真的可以使資料「去個人資料化」，非常有疑問。在歐盟個人資料保護基本規章中，有許多條文均提到「假名化」(pseudonymisation; Pseudonymisierung) 一詞²⁷，而依據歐盟個人資料保

其實就是「真正的個人資料」(基於同樣的理由，學生的學號也屬於個人資料)。經由資料交互比對，可以從悠遊卡卡號得知其代表的是哪一位學生，以及該位學生在何年何月何日何時於何處購買了何物。

²⁷ 例如第 6 條第 4 項第 5 款、第 25 條第 1 項、第 32 條第 1 項第 1 款等。

護基本規章第 4 條第 5 款的定義，「假名化」這個概念是指，將個人資料作如下方式之處理：在不使用額外資訊的情況下，個人資料不再能被歸屬到特定當事人，而前提是，當該額外資訊被分開保存並且採取技術及組織上之措施，確保個人資料不會被歸屬到已遭識別或可得識別之自然人。很明顯地，歐盟個人資料保護基本規章所稱之「假名化」，其實只是將個人資料與其他額外資訊「去連結化」而已，一旦將資料重新連結額外資訊，仍可識別出特定個人，因此個人資料在「假名化」處理之後，依然具有個人資料的性質²⁸。至於「匿名化」(anonymization; Anonymisierung)，這個在歐盟個人資料保護基本規章中未見定義的概念²⁹，則是指將個人資料處理到不能或不再能從中識別出特定個人。由於「匿名化」乃是將個人資料「可識別特定個人」的性質去除，因此個人資料一旦經過「匿名化」處理，便不再是個人資料，從而不在個人資料保護相關法規的適用範圍內³⁰。

²⁸ 張陳弘、莊植寧，新時代之個人資料保護法制：歐盟 GDPR 與臺灣個人資料保護法的比較說明，2019 年，頁 27；Stefan Ernst, in: Boris P. Paal/Daniel A. Paul (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar, 2. Aufl., 2018, Art. 4 DS-GVO Rn. 40; Peter Gola, in: Peter Gola (Hrsg.), Datenschutz-Grundverordnung Kommentar, 2. Aufl., 2018, Art. 4 Rn. 39 f.; Marit Hansen, in: Spiros Simitis/Gerrit Hornung/Indra Spiecker genannt Döhmman (Hrsg.) Datenschutzrecht Kommentar, 2019, Art. 4 Nr. 5 DS-GVO Rn. 21; Achim Klabunde, in: Eugen Ehmann/Martin Selmayr (Hrsg.), Datenschutz-Grundverordnung Kommentar, 2. Aufl., 2018, Art. 4 Rn. 32 f.; Manuel Klar/Jürgen Kühling, in: Jürgen Kühling/Benedikt Buchner (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar, 2. Aufl., 2018, Art. 4 Nr. 5 DS-GVO Rn. 11; Thilo Weichert, in: Wolfgang Däubler/Peter Wedde/Thilo Weichert/Imke Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu Kommentar, 2018, Art. 4 DS-GVO Rn. 71. 不同見解則認為，對於無從支配額外資料者而言，經假名化處理之資料即非個人資料，參見：Martin Eßer, in: Martin Eßer/Philipp Kramer/Kai von Lewinski (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz und Nebengesetze Kommentar, 6. Aufl., 2018, Art. 4 DS-GVO Rn. 70.

²⁹ 德國聯邦個人資料保護法 (Bundesdatenschutzgesetz) 舊法 (適用至 2018 年 5 月 24 日) 第 3 條第 6 項則對「匿名化」概念設有立法定義。

³⁰ 張陳弘、莊植寧，前註 28，頁 27-28；Ernst (Fn. 28), Art. 4 DS-GVO Rn. 48 f.; Eßer (Fn. 28), Art. 4 DS-GVO Rn. 71; Gola (Fn. 28), Art. 4 Rn. 41; Hansen (Fn. 28), Art. 4 Nr. 5 DS-GVO Rn. 23; Klabunde (Fn. 28), Art. 4 Rn. 33; Klar/Kühling (Fn. 28), Art. 4 Nr. 1 DS-GVO Rn. 31; Weichert (Fn. 28), Art. 4 DS-GVO Rn. 79. 資訊作業實務上常見的對個人資料進行「加密」，則既非「假名化」，也非「匿名化」(Klabunde (Fn. 28), Art. 4 Rn. 34.)，但學說上也有不同見解認為，「加密」乃是

至於我國個人資料保護法的「去識別化處理」，在第 6 條第 1 項但書第 4 款、第 9 條第 2 項第 4 款、第 16 條但書第 5 款、第 19 條第 1 項第 4 款及第 20 條第 1 項但書第 5 款稱之為「無從識別特定當事人」，而依據個人資料保護法施行細則第 17 條的定義，個人資料保護法上開條文所稱「無從識別特定當事人」，是指「個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者」。很明顯地，我國個人資料保護法的「去識別化處理」，其實只是將個人資料進行「去連結化」的處理，讓人們無法從該資料「直接識別」特定個人而已。在這樣的「去識別化處理」標準下，被「去識別化處理」（其實是「去連結化處理」）的個人資料，仍能透過和「代碼對照表」、「匿名對照表」等資料相結合比對，而間接識別特定個人。既然透過該資料（間接）識別特定個人的可能性並未消除，所以就算對個人資料作了符合我國個人資料保護法標準的「去識別化處理」，該筆個人資料仍可能因為具有間接識別特定個人的功能，而還繼續保有個人資料的性質³¹。基於這樣的理由，行政機關蒐集「經去識別化處理後的個人資料」，雖然該資料已經作了（符合我國個人資料保護法標準的）去識別化處理，但行政機關所為之資料蒐集措施，仍可能對資訊隱私權構成干預效果。

參、行政機關蒐集個人資料之合法性要求

個人資料保護法第 5 條規定蒐集、處理或利用個人資料應遵守之一般原則，第 6 條但書規定蒐集、處理或利用特種個人資料³²之容許要件，第 15 條第 1 項規定公務機關蒐集一般個人資料之容許要件。這些條文之規定，共同構成公務機關蒐集個人資料之合法性要求。行政機關作為個人資料保護法所稱之公務機關³³，

一種「假名化」，參見：*Klar/Kühling* (Fn. 28), Art. 4 Nr. 5 Rn. 9.

³¹ 相同見解：范姜真燄、劉定基、李寧修，法務部「歐盟及日本個人資料保護立法最新發展之分析報告」委託研究案成果報告，2016 年 12 月，頁 151。

³² 亦即個人資料保護法第 6 條規定之「病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料」。

³³ 個人資料保護法所稱之公務機關，依據個人資料保護法第 2 條第 7 款之定義，係指「依法行

在蒐集個人資料時，自應符合個人資料保護法上開條文規定之容許要件。

一、須具有特定蒐集目的

個人資料保護法第 15 條第 1 項規定，公務機關蒐集個人資料，應有特定目的。公務機關在蒐集個人資料時，必須具有特定蒐集目的，這一項合法性要求，對於判斷其他合法性要求是否被確實遵守而言，可說是非常重要的連接點。首先，個人資料保護法第 5 條規定個人資料之蒐集、處理與利用「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」，明文規範在個人資料保護法中具有核心重要地位的「目的拘束原則」(*Grundsatz der Zweckbindung*)³⁴。如果公務機關對於個人資料之蒐集，一開始就欠缺特定蒐集目的，純粹為了蒐集而蒐集，則根本不可能判斷其採取的蒐集措施本身以及後續對於個人資料的處理與利用是否「逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯」。再者，依據個人資料保護法第 8 條第 1 項第 2 款及第 9 條第 1 項之規定，公務機關在直接向當事人蒐集個人資料時，或處理、利用間接蒐集之個人資料（亦即非由當事人提供之個人資料）時，應向當事人告知蒐集之目的，並使當事人得以告知內容為基礎，表示同意與否（個人資料保護法第 7 條）。若公務機關在蒐集個人資料時，並無特定之蒐集目的，當然不可能將蒐集目的告知當事人，當事人從而無法以完整的告知資訊作為基礎決定同意與否，對於公務機關而言，也就難以將「當事人同意」當成個人資料蒐集、處理或目的外利用之容許要件（個人資料保護法第 15 條第 2 款、第 16 條但書第 7 款）。另外，公務機關蒐集個人資料之特定目的一旦達成，原則上即應刪除、停止處理或利用該個人資料（個人資料保

使公權力之中央或地方機關或行政法人」。

³⁴ 個人資料保護法第 16 條也規定公務機關利用個人資料，原則上必須「與蒐集之特定目的相符」，同樣屬於對目的拘束原則之宣示。關於目的拘束原則的重要地位，詹鎮榮教授認為其乃具有憲法位階之誡命（詹鎮榮，前註 9，頁 11），而李惠宗教授則認為其係個人資料保護法上的帝王條款（李惠宗，目的拘束原則—個人資料保護法上的帝王條款，載於：法令月刊，第 64 卷第 1 期，2013 年 1 月，頁 37 以下）。

護法第 11 條第 3 項)。如果公務機關在蒐集個人資料時欠缺特定目的，也就難以判斷公務機關在法律上應刪除、停止處理或利用該個人資料的時間點。

公務機關蒐集個人資料之特定目的，一方面為其蒐集、處理、利用個人資料提供了正當性基礎，另一方面也劃定其蒐集、處理、利用個人資料的界限³⁵。也正因為如此，所以雖然個人資料保護法第 15 條僅簡單提到「應有特定目的」，但在解釋上，該「特定目的」本身應該要如同歐盟個人資料保護基本規章第 5 條第 1 項第 2 款的要求一樣，必須是「正當」(legitimate)且「明確」(explicit)之特定目的³⁶。公務機關蒐集個人資料，如果是以不正當之目的作為出發點，那麼其對資訊隱私權造成的干預，便已經可以確定違憲，無須再檢視手段與目的之間的關係如何。公務機關蒐集個人資料之特定正當目的，同時還必須符合明確性之要求。有鑑於蒐集個人資料的目的本身，乃是判斷個人資料保護法其他合法性要求是否被確實遵守的基礎所在，所以蒐集個人資料之目的本身是否詳細明確，應該要從嚴認定³⁷。而且，公務機關蒐集的個人資料愈具有敏感性，那麼對於「目的明確性」的要求程度也就愈高³⁸。如果蒐集個人資料之目的，概括模糊到足以包含諸多可能的目的在內，那麼一方面該目的本身已經不是「特定」目的³⁹，另一方面公務機關基於此等（模糊）目的蒐集個人資料，也已違反目的拘束原則⁴⁰。

行政機關作為受個人資料保護法第 15 條拘束之公務機關，由於在「蒐集資料時」就必須具有特定、正當、明確之目的，因此不得對個人資料採取儲備性(auf

³⁵ Alexander Roßnagel, in: Alexander Roßnagel (Hrsg.), *Das neue Datenschutzrecht*, 2018, § 3 Rn. 63.

³⁶ 相同結論：洪家殷，公務機關資料之蒐集與個人資料之保護，載於：東吳法律學報，第 30 卷第 4 期，2019 年 4 月，頁 46。

³⁷ Philipp Kramer, in: Martin Eßer/Philipp Kramer/Kai von Lewinski (Hrsg.), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz und Nebengesetze Kommentar*, 6. Aufl., 2018, Art. 5 DS-GVO Rn. 19 f.; Roßnagel (Fn. 35), § 3 Rn. 65.

³⁸ Weichert (Fn. 28), Art. 5 DS-GVO Rn. 36.

³⁹ Stephan Pötters, in: Peter Gola (Hrsg.), *Datenschutz-Grundverordnung Kommentar*, 2. Aufl., 2018, Art. 5 Rn. 14.

⁴⁰ Roßnagel (Fn. 35), § 3 Rn. 64.

Vorrat) 之蒐集與儲存⁴¹，也就是說，行政機關若基於模糊不確定之目的蒐集個人資料並待將來有朝一日再基於確定之目的予以利用，便違反「蒐集個人資料必須有特定目的」的要求⁴²。另外，基於行政一體原則⁴³，行政機關依據行政程序法第 19 條第 1 項之規定，應於權限範圍內相互協助。但是，由於行政機關在蒐集個人資料時必須具有特定目的，且後續對於個人資料之利用也不得逾越該特定目的範圍，所以在目的拘束原則的要求下，關於個人資料之蒐集與利用，並無行政一體原則以及行政機關職務協助相關規定之適用⁴⁴。行政機關不能以行政一體或職務協助為名，要求其他機關向本機關提供個人資料俾便本機關利用，或將本機關蒐集之個人資料提供其他機關任意利用⁴⁵，否則個人資料保護法上之目的拘束原則，將被機關間的職務協助徹底架空，也使個人資料當事人無從預見其基於特定目的被蒐集之個人資料，未來會被蒐集機關提供給哪一個機關作何種目的之利用，而使個人資料當事人失去對其個人資料之自主決定地位。

二、經當事人同意

個人資料保護法第 15 條第 2 款將「經當事人同意」列為公務機關蒐集個人資料的容許要件之一，而同法第 6 條第 1 項但書第 6 款也將「經當事人書面同意」列為得例外蒐集、處理、利用特種個人資料之要件。由於資訊隱私權的核心內涵，

⁴¹ 洪家殷，同註 36，頁 48。

⁴² *Horst Heberlein*, in: Eugen Ehmann/Martin Selmayr (Hrsg.), *Datenschutz-Grundverordnung Kommentar*, 2. Aufl., 2018, Art. 4 Rn. 13; *Alexander Roßnagel*, in: Spiros Simitis/Gerrit Hornung/Indra Spiecker genannt Döhmann (Hrsg.) *Datenschutzrecht Kommentar*, 2019, Art. 5 DS-GVO Rn. 72.

⁴³ 大法官在司法院釋字第 603 號解釋理由書中，從憲法第 53 條之規定導出行政一體原則，並指出：「行政必須有整體之考量，無論如何分工，最終仍須歸屬最高行政首長統籌指揮監督，方能促進合作，提昇效能，並使具有一體性之國家有效運作，此即所謂行政一體原則」。

⁴⁴ *Weichert* (Fn. 28), Art. 5 DS-GVO Rn. 30.

⁴⁵ 詹鎮榮教授則認為，有取得資訊需求之行政機關，仍得依據行政程序法第 19 條第 2 項之規定，向其他機關提出資訊上之職務協助請求，但被請求機關對於該職務協助請求，應以個人資料保護法之合法性要件為據，決定同意或拒絕。參見：詹鎮榮，同註 9，頁 16。

乃在確保每個人對其個人資料的自主決定地位，因此一旦當事人(基於自由意願)同意行政機關蒐集、處理、利用其個人資料，則該個人資料蒐集措施對於資訊隱私權就沒有構成干預效果⁴⁶，既然不構成基本權干預，當然也就無須有法律授權依據作為基本權干預的形式阻卻違憲事由⁴⁷。

三、對當事人權益無侵害

個人資料保護法第 15 條第 3 款將「對當事人權益無侵害」列為與第 2 款「經當事人同意」平行適用之容許要件。因此，在未經當事人同意的情況下，行政機關仍得單獨以「對當事人權益無侵害」為由蒐集個人資料。然而，在未經當事人同意的情況下蒐集個人資料，姑且不論其他權利，至少已經對資訊隱私權造成干預，根本不可能「對當事人權益無侵害」，所以個人資料保護法第 15 條第 3 款的適用可能性實在難以想像⁴⁸。

四、執行法定職務

除了(適用可能性殊難想像的)「對當事人權益無侵害」(個人資料保護法第 15 條第 3 款)之外，「執行法定職務必要範圍內」也被個人資料保護法列為與「經

⁴⁶ 「當事人同意」在憲法上的意義，乃是人民對於資訊隱私權(個人資訊自主決定權)的「行使」(相同結論：洪家殷，同註 36，頁 49)。劉定基教授對此也認為，「當事人同意權」乃是「實現資訊隱私保護，落實個人資料自主控制最為直接的手段」(劉定基，析論個人資料保護法上「當事人同意」的概念，載於：月旦法學雜誌，第 218 期，2013 年 6 月，頁 147)。不過，詹鎮榮教授則認為，「當事人同意」在憲法上的意義，乃是人民對於基本權(資訊隱私權)的「拋棄」。參見：詹鎮榮，同註 9，頁 13。

⁴⁷ Jarass (Fn. 12), Art. 2 Rn. 54; Philipp Reimer, Verwaltungsdatenschutzrecht, 2019, Rn. 148. 但也有學者認為，就算經當事人同意，仍然構成基本權之干預，只不過該基本權干預會因為「當事人同意」而阻卻違憲，參見：Dreier (Fn. 12), Art. 2 I Rn. 90; Hufen (Fn. 12), § 11 Rn. 22.

⁴⁸ 相同見解：張陳弘、莊植寧，前註 28，頁 106-107。范姜真燮教授更認為，個人資料保護法第 15 條第 3 款被行政機關濫用的可能性極高，參見：范姜真燮，檢視行政機關蒐集利用個資之問題與展望，載於：法學叢刊，第 63 卷第 2 期，2018 年 4 月，頁 37-38。

當事人同意」平行適用的公務機關蒐集個人資料容許要件（個人資料保護法第 15 條第 1 款）。此外，依據個人資料保護法第 16 條之規定，「執行法定職務必要範圍內」亦屬公務機關利用個人資料之合法要件⁴⁹。對於行政機關而言，其法定職務乃是被法律交付應履行之公共任務，也就是說，乃是行政機關之法定管轄事務。由於行政機關之事務管轄係規定於機關的組織法，所以最高行政法院 106 年度判字第 54 號判決（健保資料庫案確定判決）認為，個人資料保護法所稱之「法定職務」即是組織法規定之執掌事項，從而在個人資料保護法第 15 條第 1 款以及第 16 條的肯認下，行政機關得以機關之組織法作為蒐集個人資料之法律依據⁵⁰。

就本文看來，最高行政法院 106 年度判字第 54 號判決上開見解的說服力，恐怕有待商榷。個人資料保護法第 15 條第 1 款以及第 16 條的規範文字，並非（僅是）「法定職務」，而是「執行法定職務」。一方面，行政機關的「職務」本身，在行政程序法第 11 條第 1 項「管轄法定原則」的制約下，就如同個人資料保護

⁴⁹ 在比較法上，歐盟個人資料保護基本規章和我國個人資料保護法的規範體例不同，其一方面並未將拘束對象區分成「公務機關」與「非公務機關」，而是區分成「責任人」（*controller; Verantwortlicher*）與「受託處理人」（*processor; Auftragsverarbeiter*），另一方面也並未將規範之行為階段區分個人資料之蒐集、處理與利用，而是以「處理」（*processing; Verarbeitung*）概念統稱之（*Charlotte Husemann, in: Alexander Roßnagel (Hrsg.), Das neue Datenschutzrecht, 2018, § 3 Rn. 3 ff.*）。雖然有如此規範體例之差異，但我國個人資料保護法第 15 條第 1 款以及第 16 條的「執行法定職務必要範圍內」要件，在歐盟個人資料保護基本規章倒是可以找得到相類似的規定。歐盟個人資料保護基本規章第 6 條規定「處理之合法性」（*Lawfulness of processing; Rechtmäßigkeit der Verarbeitung*），其第 1 項第 5 款將「履行公共利益任務或公權力任務而有必要」列為處理個人資料的合法要件之一，即與我國個人資料保護法第 15 條第 1 款以及第 16 條的「執行法定職務必要範圍內」類似，且此一合法要件顯然係為公部門而設（*Philipp Reimer, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung Kommentar, 2. Aufl., 2018, Art. 6 Rn. 36; Sebastian Schulz, in: Peter Gola (Hrsg.), Datenschutz-Grundverordnung Kommentar, 2. Aufl., 2018, Art. 60 Rn. 48; Peter Wedde, in: Wolfgang Däubler/Peter Wedde/Thilo Weichert/Imke Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu Kommentar, 2018, Art. 6 DS-GVO Rn. 87*）。

⁵⁰ 參見：最高行政法院 106 年度判字第 54 號判決，判決理由「八、（二）、2、（2）」。

法第 15 條第 1 款以及第 16 條的規範文字所稱，必須是「法定職務」，也就是說，其管轄事務必須於法有據。另一方面，行政機關對其「法定職務」之「執行」，也同樣必須符合依法行政原則。無論是行政機關的「職務」，抑或是行政機關職務之「執行」，在依法行政原則的要求下，均須具備合法性。因此，個人資料保護法第 15 條第 1 款以及第 16 條所稱「執行法定職務」，說得更精確一點，其實指的是「合法執行法定職務」⁵¹。行政機關執行法定職務要具備合法性，除了不得牴觸法律之規定(法律優位原則)，還必須具有法律授權依據(法律保留原則)。關於行政機關蒐集個人資料之法律依據，大法官在司法院釋字第 553 號解釋闡述「警察臨檢」的合憲性問題時，於該號解釋理由書清楚指出：「行政機關行使職權，固不應僅以組織法有無相關職掌規定為準，更應以行為法(作用法)之授權為依據，始符合依法行政之原則」。在司法院釋字第 553 號解釋理由書清楚的闡述下，行政機關執行職務，該「職務」在組織法上有相關職掌規定，這只是最基本的前提而已，至於組織法上的職務應採取何種措施來「執行」，則還必須進一步以行為法(作用法)性質的法律作為授權依據⁵²。也正因為如此。所以個人資料保護法第 15 條第 1 款以及第 16 條的「執行法定職務」規定，本身並沒有什麼

⁵¹ 歐盟個人資料保護基本規章第 6 條第 1 項第 5 款的「履行任務」(請見前註 49)，也同樣被理解為「合法履行任務」。因應歐盟個人資料保護基本規章之生效施行，德國全盤翻修聯邦個人資料保護法。自 2018 年 5 月 25 日正式生效施行的(新版)德國聯邦個人資料保護法，其第 3 條規定「公部門履行管轄權任務或公權力任務而有必要，得處理個人資料」，完全將歐盟個人資料保護法第 6 條第 1 項第 5 款的條文內容(請見前註 49)予以複製。德國學者在詮釋該國聯邦個人資料保護法第 3 條的「公部門履行任務」時，也同樣區分「任務(管轄權)本身之合法性」以及「任務履行之合法性」兩個不同層次的問題，參見：*Tobias Starnecker*, in: *Peter Gola/Dirk Heckmann* (Hrsg.), *Bundesdatenschutzgesetz Kommentar*, 13. Aufl., 2019, § 3 Rn. 22; *Wedde* (Fn. 49), § 3 BDSG Rn. 8 ff.

⁵² 相同結論：范姜真嫻，同註 48，頁 37；詹鎮榮，同註 9，頁 13。張陳弘教授對此則持不同見解，認為行政機關蒐集個人資料保護法第 6 條之特種個人資料，固然必須有作用法性質之法律作為授權依據，但如果蒐集的是一般個人資料，則可拿個人資料保護法之規定當成作用法之依據。參見：張陳弘，國家建置全民健康保險資料庫之資訊隱私保護爭議－評最高行政法院 106 年度判字第 54 號判決，載於：中原財經法學，第 40 期，2018 年 6 月，頁 23。

實質上的規範意義⁵³，只不過是再次重申「公務機關蒐集處理、利用個人資料，應有組織法及行為法之法律授權依據」此一依法行政原則的精神罷了，更不可能被拿來當作公務機關蒐集、處理、利用個人資料的法律授權依據⁵⁴。最高行政法院 106 年度判字第 54 號判決認為個人資料保護法第 15 條第 1 款以及第 16 條的「執行法定職務」規定允許行政機關得以組織法為依據蒐集、處理、利用個人資料，此等見解顯然忽略了條文中的「執行」二字，並將組織法與行為法的規範性質混淆在一起⁵⁵，當然，也違反了司法院釋字第 535 號解釋的意旨⁵⁶。

⁵³ 相同見解：張陳弘、莊植寧，前註 28，頁 106。

⁵⁴ 德國自 2018 年 5 月 25 日正式生效施行的（新版）聯邦個人資料保護法，其第 3 條關於「公部門履行任務」之規定（請見前註 51），則被立法理由承認可以作為公部門處理（亦即包括我國個人資料保護法的蒐集、處理、利用）個人資料的法律依據，但僅限於對當事人權利造成「輕微」干預的場合（BT-Drs. 18/11325, S. 81）。若公部門所為之個人資料處理行為，對當事人權利之干預程度非屬「輕微」，則仍應有具體明確之專業法律規定作為授權依據始得為之，不得援引聯邦個人資料保護法第 3 條之概括規定作為法律依據（*Thomas Petri*, in: Jürgen Kühling/Benedikt Buchner (Hrsg.), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar*, 2. Aufl., 2018, § 3 BDSG Rn. 9; *Starnecker* (Fn. 51), § 3 Rn. 22)。對於德國聯邦個人資料保護法第 3 條立法理由承認公部門得以本條作為處理個人資料之法律依據，有德國學者提出批評，認為德國聯邦個人資料保護法第 3 條就如同歐盟個人資料保護基本規章第 6 條第 1 項第 5 款一樣，本身都是空洞沒有實質內容的規範，公部門若要以「履行公共任務」為由處理（包括蒐集、利用）個人資料，仍須進一步在擁有具體規範內容的其他專業法規中，分別針對「公共任務」以及「公共任務之履行」找到法律依據才行（*Eßer* (Fn. 28), § 3 BDSG Rn. 5; 相同結論：*Wedde* (Fn. 49), § 3 BDSG Rn. 10）。

⁵⁵ 組織法賦予行政機關對某行政事務具有管轄權，乃在劃分該機關與其他機關之間的權限分際，亦即以「機關與機關之間的法律關係」為規範內容；至於行為法（作用法），則係規定行政機關得在如何之要件下對何等對象採取何種措施，亦即以「機關與人民之間的法律關係」為規範內容。

⁵⁶ 最高行政法院雖非司法院釋字第 535 號解釋的「當事人」，但基於司法院解釋的「一般效力」（司法院釋字第 185 號解釋：「司法院解釋憲法，並有統一解釋法律及命令之權，為憲法第七十八條所明定，其所為之解釋，自有拘束全國各機關及人民之效力，各機關處理有關事項，應依解釋意旨為之」），亦同樣受司法院釋字第 535 號解釋拘束。「行政機關行使職權，固不應僅以組織法有無相關職掌規定為準，更應以行為法（作用法）之授權為依據，始符合依法行政之原則」這一段文字，乃是構成司法院釋字第 535 號解釋結論（警察勤務條例具有行為法之性質，故可作為警察臨檢之法律授權依據，但條文必須符合法明確性原則）的重要理由部分，因此雖然未見諸解釋文（只寫在解釋理由書），但其對各機關（包括最高行政法院）之拘束力應無庸置疑。

五、必要性

個人資料保護法第 15 條第 1 款規定之公務機關蒐集個人資料合法要件，由兩個構成要件要素共同組成，其一是前述的「執行法定職務」，其二則是「必要範圍」，也就是執行法定職務的「必要性」。另外，個人資料保護法第 5 條、第 6 條第 1 項第 2 款、第 4 款、第 5 款、第 16 條前段、第 16 條但書第 2 款、第 5 款也將「必要性」列為公務機關蒐集、處理、利用個人資料的合法要件要素。

一提到「必要性」，很多人可能會馬上聯想到憲法第 23 條透過「必要」二字揭櫫之比例原則，並因此將個人資料保護法各該條文中的「必要」二字理解為「符合比例原則之要求」⁵⁷。行政機關蒐集、處理、利用個人資料，乃是對資訊隱私權構成干預效果之行政行為，無論從憲法第 23 條抑或是從行政程序法第 7 條來看，當然必須符合比例原則的要求，這一點無庸置疑。然而，本文必須強調，個人資料保護法各該條文所稱之「必要」，指的並不是比例原則，而是獨立於比例原則之外的另一項要求。歐盟個人資料保護基本規章第 5 條第 1 項第 3 款規定，被處理之個人資料應屬對目的而言適當且相關之資料，並應僅止於處理目的之必要限度內。此一規定被歐盟個人資料保護基本規章直接定名為「資料最小化原則」（data minimisation; Datenminimierung）。我國個人資料保護法第 5 條「個人資料之蒐集、處理或利用，...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」的規定，與歐盟個人資料保護基本規章第 5 條第 1 項第 3 款的

⁵⁷ 採此見解者：林洲富，個人資料保護法之理論與實務，2 版，2019 年 10 月，頁 26-27；張陳弘、莊植寧，前註 28，頁 69-70。至於最高行政法院 106 年度判字第 54 號判決（健保資料庫案確定判決），則引用衛生福利部組織法之相關規定確定衛生福利部的職權範圍後，認為健保資料庫之建置，「有助於其執掌事項之踐行，...因此建置上開資料庫，同樣在其『執行法定職務』之必要範圍內」（請參見：最高行政法院 106 年度判字第 54 號判決，判決理由「八、(二)、2、(2)」）。依照最高行政法院 106 年度判字第 54 號判決的論理，本號判決似乎是將「必要」二字理解為比例原則中的「適當性原則」（手段有助於目的之達成）。

內容大致相同，被認為是「資料最小化原則」在我國的實定法依據⁵⁸。須特別提請注意的是，資料最小化原則所稱「被蒐集、處理、利用之資料，應僅止於蒐集、處理、利用目的必要限度內之資料」，係指若不蒐集、處理、利用該個人資料，則欲達成之目的即無法達成⁵⁹。對於行政機關而言，在資料最小化原則的制約下，個人資料保護法各該條文所稱之「必要」，其意義並非「符合比例原則」，更非「符合適當性原則」⁶⁰，而是「絕對必要」⁶¹，也就是說，若不蒐集、處理、利用個人資料，則行政機關欲達成之目的即無法達成，基於該目的而產生之法定職務即無法（有效）履行⁶²。也正因為如此，所以行政機關將個人資料作「儲備性儲存」，不但違反「蒐集個人資料之目的必須特定、正當、明確」的要求⁶³，也與蒐集、處理、利用個人資料之「必要性」要求不符⁶⁴。

六、尊重當事人之權益

個人資料保護法在諸多條文中，明文保障個人資料當事人之請求權，例如個人資料保護法第 10 條保障「請求查詢或閱覽之權利」，第 11 條各項分別保障「請求更正、補充、刪除、停止蒐集、處理之權利」。這些在個人資料保護法中明文

⁵⁸ 張陳弘、莊植寧，前註 28，頁 70（但該書稱之為「最少蒐集原則」）。

⁵⁹ Heberlein (Fn. 42), Art. 5 Rn. 22; Roßnagel (Fn. 42), Art. 5 DS-GVO Rn. 121.

⁶⁰ 但最高行政法院 106 年度判字第 54 號判決似乎認為個人資料保護法中的「必要」二字，僅是「適當性原則」（手段有助於目的之達成）的要求而已，請參見前註 57。

⁶¹ Heberlein (Fn. 42), Art. 6 Rn. 23; Petri (Fn. 54), § 3 BDSG Rn. 14; Roßnagel (Fn. 42), Art. 6 As. 1 DS-GVO Rn. 77; Starnecker (Fn. 51), § 3 Rn. 28.

⁶² Eßer (Fn. 28), § 3 BDSG Rn. 21; Petri (Fn. 54), § 3 BDSG Rn. 14; Reimer (Fn. 49), Art. 6 Rn. 47; Roßnagel (Fn. 42), Art. 5 DS-GVO Rn. 121; Lutz Schreiber, in: Kai-Uwe Plath (Hrsg.), Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG, 3. Aufl., 2018, § 3 BDSG Rn. 7; Starnecker (Fn. 51), § 3 Rn. 28; Wedde (Fn. 49), § 3 BDSG Rn. 13. 但也有不同見解認為，在「資料最小原則」下，「必要性」指的就是符合比例原則：Eike Michael Frenzel, in: Boris P. Paal/Daniel A. Paul (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar, 2. Aufl., 2018, Art. 6 DS-GVO Rn. 23; Kramer (Fn. 37), Art. 5 DS-GVO Rn. 26.

⁶³ 請見前註 42。

⁶⁴ Eßer (Fn. 28), § 3 BDSG Rn. 32.

受到保障的當事人權利，乃是資訊隱私權（個人資料自主決定權）之進一步具體化，且依個人資料保護法第 3 條之規定，不得預先拋棄或以特約限制之。同時，個人資料保護法第 5 條也規定，個人資料之蒐集、處理或利用，應尊重當事人之權益。基於個人資料保護法上開各條之規定，行政機關對於受個人資料保護法明文保障之各種請求權，應予尊重。

行政機關在行政程序進行中，為了作成實體決定而蒐集、處理、利用個人資料，個人資料當事人對於行政機關這樣的行為，在行政程序進行中向行政機關主張前揭個人資料保護法保障之當事人權利，可能會遭到行政機關依據個人資料保護法第 10 條但書各款或第 11 條第 2 項但書、第 3 項但書等規定予以拒絕。無論行政機關在行政程序進行中對個人資料所為之蒐集、處理、利用行為，抑或是行政機關在行政程序進行中對個人資料當事人所為之拒絕決定，均屬於行政程序法第 174 條⁶⁵所稱「行政機關於行政程序中所為之決定或處置」，亦即學理上所稱之「程序行為」（*Verfahrenshandlungen*）⁶⁶。由於行政機關在行政程序進行中對個人資料所為之蒐集、處理、利用行為，以及行政機關在行政程序進行中對個人資料當事人所為之拒絕決定，都不符合行政程序法第 174 條但書之要件⁶⁷，因此依據行政程序法第 174 條，個人資料當事人似乎不能單獨針對此等程序行為提起行政爭訟，必須等到行政程序終結後，始得與實體決定一併聲明不服。

不過，本文認為，上開結論的正確性恐怕有待商榷。司法院釋字第 665 號解釋理由書指出，憲法第 16 條保障之訴訟權，「其核心內容在於人民之權益遭受侵

⁶⁵ 德國行政法院法（*Verwaltungsgerichtsordnung, VwGO*）第 44 條之 1，其規範內容與我國行政程序法第 174 條相同。

⁶⁶ 吳庚、盛子龍，*行政法之理論與實用*，15 版，2017 年 9 月，頁 591；陳敏，*行政法總論*，9 版，2016 年 9 月，頁 833；*Steffen Detterbeck, Allgemeines Verwaltungsrecht, 17. Aufl., 2019, Rn. 960; Hartmut Maurer/Christian Waldhoff, Allgemeines Verwaltungsrecht, 19. Aufl., 2017, § 19 Rn. 41.*

⁶⁷ 依據行政程序法第 174 條但書，行政機關之程序行為若得強制執行，或行政程序法以及其他法規設有容許規定，則程序當事人或利害關係人即得在行政程序進行中，對該程序行為提起行政爭訟。

害時，得請求法院依正當法律程序公平審判，以獲得及時有效之救濟」。大法官在後續多號司法院解釋（理由書）中，也持續強調憲法第 16 條訴訟權之保障內涵乃是「及時有效救濟」⁶⁸。行政程序法第 174 條之規定，為了行政程序順利進行之目的⁶⁹，禁止人民在行政程序進行中針對程序行為提起行政爭訟，使人民無法「及時」向法院尋求救濟，已經碰觸到憲法第 16 條訴訟權的保障核心。既然行政程序法第 174 條的規定，已觸及訴訟權保障的核心領域，那麼為了避免行政程序法第 174 條的規定違反憲法第 16 條之訴訟權保障，應該要對行政程序法第 174 條採取合憲性解釋（*verfassungskonforme Auslegung*）⁷⁰。基於這樣的考量，在解釋行政程序法第 174 條的「程序行為」時，必須採取較為限縮的立場⁷¹，將「對實體權利（尤其是基本權）構成單獨干預效果之程序行為」排除在行政程序法第 174 條的適用範圍外⁷²。就此而言，行政機關所為之程序行為，如果對人民受憲法保障的資訊隱私權（資訊自主權決定權）造成干預，應該要允許人民得針對該基本權干預行為「及時」提起行政爭訟尋求救濟，不受行政程序法第 174 條拘束⁷³。因此，行政機關在行政程序進行中對個人資料所為之蒐集、處理、利

⁶⁸ 參見司法院釋字第 736 號解釋理由書、第 742 號解釋理由書、第 752 號解釋理由書、第 755 號解釋理由書、第 761 號解釋理由書、第 774 號解釋理由書、第 784 號解釋理由書。

⁶⁹ 吳庚、盛子龍，前註 66，頁 591-592；陳敏，前註 66，頁 833。

⁷⁰ 德國學者闡述該國行政法院法第 44 條之 1 時的相同主張：*Klaus F. Gärditz*, in: Klaus F. Gärditz (Hrsg.), *Verwaltungsgerichtsordnung mit Nebengesetz Kommentar*, 2. Aufl., 2018, § 44a VwGO Rn. 19; *Wolf-Rüdiger Schenke*, in: Ferdinand O. Kopp (Begr.)/Wolf-Rüdiger Schenke (Hrsg.), *Verwaltungsgerichtsordnung Kommentar*, 25. Aufl., 2019, § 44a Rn. 1; *Paul Stelkens/Wolfgang Schenk*, in: Friedrich Schoch/Jens-Peter Schneider/Wolfgang Bier (Hrsg.), *Verwaltungsgerichtsordnung Kommentar*, Werkstand: 36. EL Februar 2019, § 44a Rn. 30; *Jan Ziekow*, in: Helge Sodan/Jan Ziekow (Hrsg.), *Verwaltungsgerichtsordnung Kommentar*, 5. Aufl., 2018, § 44a Rn. 73.

⁷¹ 相近的見解：李震山，*行政法導論*，11 版，2019 年 2 月，頁 268：「就行政程序相關之決定或措施，若涉及程序基本權之核心內涵者，第一七四條之適用範圍即應受到限縮」。

⁷² *Gärditz* (Fn. 70), § 44a VwGO Rn. 21; *Schenke* (Fn. 70), § 44a Rn. 9; *Stelkens/Schenk* (Fn. 70), § 44a Rn. 32; *Ziekow* (Fn. 70), § 44a Rn. 73.

⁷³ *Schenke* (Fn. 70), § 44a Rn. 10; *Stelkens/Schenk* (Fn. 70), § 44a Rn. 32; *Ziekow* (Fn. 70), § 44a Rn. 74.

用行為，以及行政機關在行政程序進行中對個人資料當事人所為之拒絕決定，雖然都是行政機關所為之「程序行為」，但由於此等程序行為會單獨對資訊隱私權（資訊自主決定權）構成干預效果，所以不在行政程序法第 174 條的適用範圍內，當事人得在行政程序進行中，單獨針對此等程序行為提起行政爭訟以尋求「及時有效」之救濟⁷⁴。

肆、台北市政府單一識別系統之問題

台北市政府在 2019 年 9 月 20 日訂定發布「台北市政府單一識別服務作業要點」（以下稱「作業要點」），並自 2019 年 9 月 23 日生效。依據作業要點之規定，民眾得向服務機關⁷⁵之申辦窗口⁷⁶申請辦理單一識別⁷⁷服務，提交申請表（作業要點附件一）所載之個人資料，經台北市政府資訊局審核通過後成為單一識別系統⁷⁸會員（作業要點第二點（八）），並因此得透過綁定之載具⁷⁹經單一識別系統識別身分後，使用服務機關⁸⁰提供之服務。單一識別系統之統籌規劃、建置與維護，則屬台北市政府資訊局之權責（作業要點第十點）。簡單地說，作業要點所規範

⁷⁴ 相同結論：Reimer (Fn. 47), Rn. 317.

⁷⁵ 依據作業要點第二點（一）之定義，服務機關乃是提供市政服務之台北市政府所屬機關（含所屬機關（構）、學校暨台北大眾捷運股份有限公司）。

⁷⁶ 依據作業要點第二點（二）之定義，申辦窗口乃是協助服務機關受理申請人辦理服務之自然人或機關（構）。

⁷⁷ 依據作業要點第二點（五）之定義，單一識別是指：以市政服務總歸戶概念，藉由蒐集、處理申請表所載之各項市政服務用戶個人資料，統一其身分識別方式，包括使用服務機關已發行之 IC 卡證、數位憑證，或其他線上認證授權等；識別範圍包括用戶身分、現有卡證卡面資料，及各項市政服務開通或未開通之註記。

⁷⁸ 依據作業要點第二點（七）之定義，單一識別系統乃是用於管理會員之單一識別資料，執行會員身分識別之資訊系統。

⁷⁹ 依據作業要點第二點（三）之定義，載具是指用以出示身分識別之卡證或裝置設備（如 IC 卡證、手機等）。

⁸⁰ 依據作業要點第二點（一）之定義，服務機關乃是提供市政服務之台北市政府所屬機關（含所屬機關（構）、學校暨台北大眾捷運股份有限公司）。

之單一識別服務，乃是透過對民眾個人資料之蒐集，將原本各機關採用的各種身分識別機制整併到台北市政府資訊局建置的單一識別系統內，讓民眾藉由綁定之單一載具即可通過各種市政服務所必須之身分認證程序。乍看之下，單一識別系統以及單一識別服務能讓民眾使用各項市政服務時更為便利，但是，若進一步細讀作業要點的內容，則不難發現存有諸多法律上的疑問。

一、法律依據？

就本文看來，台北市政府要建置單一識別系統以及推行單一識別服務，一開始在法律上就遇到最形式，也是最根本的質疑：法律依據何在？單一識別系統的建置以及單一識別服務的運作，其基礎在於台北市政府⁸¹對單一識別資料⁸²之蒐集、處理與利用，從而涉及資訊隱私權（個人資料自主決定權）之干預。既然涉及資訊隱私權之干預，在憲法第 23 條法律保留原則的制約下，當然必須要有法律授權依據，始具備最起碼的形式阻卻違憲事由。

就法律保留原則的適用密度而言，依據大法官在司法院釋字第 443 號解釋理由書建構的「層級化保留體系」⁸³，國家限制人民受憲法第 22 條保障之基本權，屬於相對法律保留事項，應由法律親自加以規定，或在符合授權明確性的要求下，由法律授權行政機關訂定行政命令（法規命令）為補充規定。至於地方行政機關要干預從憲法第 22 條導出之資訊隱私權，在地方制度法第 28 條第 2 款的規定下，亦得以自治條例作為法律授權依據⁸⁴。

⁸¹ 關於單一識別資料之蒐集機關不明的問題，容後再述，請見本文「肆、二、(二)、1」。

⁸² 依據作業要點第二點（六）之規定，單一識別資料包括各項市政服務用戶之個人資料，以及各服務機關自訂並歸戶之現有卡證卡面資料、各項市政服務開通或未開通之註記。

⁸³ 對此詳請參見：吳庚、盛子龍，前註 66，頁 90-91；陳敏，前註 66，頁 161。

⁸⁴ 依據司法院釋字第 38 號解釋，地方立法若無法律依據，不得限制人民之權利。但是，地方制度法第 28 條第 2 款既然已經規定「限制地方自治團體居民之權利，應以自治條例定之」，那麼考量憲法對地方自治之保障，應可將地方制度法第 28 條第 2 款視為地方立法機關以自治條例限制人民權利之「法律依據」（對此持保留態度者：陳敏，前註 66，頁 164-165）。

台北市政府要建置單一識別系統以及推行單一識別服務，由於涉及憲法第 22 條資訊隱私權之限制，應該要有法律或自治條例作為法律依據（並在法律或自治條例的明確授權下訂定法規命令或自治規則為補充規定）。然而，作業要點既非法律或法律授權訂定之法規命令，也非自治條例或自治條例授權訂定之自治規則，只不過是台北市政府依職權自行訂定之行政規則而已，根本不能作為限制資訊隱私權的法律依據。再者，如前所述，無論是行政機關的組織法，抑或是行政程序法第 19 條「職務協助」之規定，均不能被行政機關當成蒐集個人資料或提供其他機關個人資料之法律依據⁸⁵。因此，一方面，台北市政府組織自治條例第 2 條第 1 項或台北市政府資訊局組織規程第 3 條之管轄事務規定，並非台北市政府蒐集單一識別資料之法律依據；另一方面，台北市政府亦不得依據行政程序法第 19 條「職務協助」之規定請求其他機關提供單一識別資料。在欠缺法律依據的情況下，台北市政府要拿僅具行政規則性質的作業要點，當作蒐集單一識別資料的法律依據，有違法律保留原則之要求。由於欠缺法律授權依據，所以台北市政府蒐集單一識別資料，若要符合個人資料保護法第 15 條的合法要求，大概也只剩下該條第 2 款「經當事人同意」一途⁸⁶。

二、當事人經明確告知而同意？

目前，台北市政府蒐集單一識別資料，最主要的途徑，乃是由民眾依據作業要點之規定，填具申請書申辦成為單一識別服務會員，並向台北市政府提供其個人資料作為單一識別資料。也就是說，台北市政府乃是經由當事人之書面同意，而蒐集個人資料，似乎符合個人資料保護法第 15 條第 2 款之要件。關於當事人同意，必須注意的是，行政機關經當事人同意而蒐集個人資料，其前提在於，行政機關已依個人資料保護法第 8 條第 1 項之規定向當事人明確告知各款事項，使

⁸⁵ 請參見本文「參、一」以及「參、四」。

⁸⁶ 至於個人資料保護法第 15 條第 3 款，其適用可能性殊難想像，請見本文「參、三」。

當事人能以充分之資訊作為判斷基礎，按其自由意願決定是否同意提供個人資料給行政機關⁸⁷。就此而言，台北市政府經當事人書面同意而蒐集單一識別資料，便存在兩個環環相扣的問題：（一）首先，台北市政府在得到當事人同意前，能否豁免個人資料保護法第 8 條第 1 項之告知義務？（二）其次，若台北市政府仍須踐行個人資料保護法第 8 條第 1 項之告知義務，其告知內容是否明確？若台北市政府未踐行告知義務，或雖已踐行告知義務，但告知內容卻不明確，那麼就算當事人已表示同意，該同意之意思表示也不符合個人資料保護法第 7 條對於「同意」之定義，台北市政府從而不能以「經當事人同意」作為蒐集以及後續處理、利用個人資料之法律容許事由。

（一）告知義務之豁免？

行政機關蒐集個人資料，若有個人資料保護法 8 條第 2 項各款情形，得豁免告知當事人之義務⁸⁸。就台北市政府蒐集單一識別資料而言，並無法律規定得豁免告知義務，告知也不會對台北市政府執行法定職務或公共利益造成妨害，當事人對於應告知之內容（其哪些個人資料將被哪些機關拿去在何等期間內作何種用途使用）並不知情，因此和個人資料保護法第 8 條第 2 項第 1 款、第 3 款、第 4 款以及第 5 款無關。由於台北市政府蒐集單一識別資料，並無法律授權依據，所以也不符合個人資料保護法第 8 條第 2 項第 2 款（執行法定職務）之豁免要件。至於個人資料保護法第 8 條第 2 項第 6 款，也不適用於台北市政府蒐集單一識別資料之情形。個人資料保護法第 8 條第 2 項第 6 款所稱「對當事人顯無不利之影響」，就如同該法第 15 條第 3 款「對當事人權益無侵害」一樣，有鑑於個人資料

⁸⁷ 對此更進一步的說明，參見：洪家殷，同註 36，頁 49-50；張陳弘，新興科技下的資訊隱私保護：「告知後同意原則」的侷限性與修正方法之提出，載於：臺大法學論叢，第 47 卷第 1 期，2018 年 3 月，頁 214 以下；劉定基，前註 46，頁 156 以下。

⁸⁸ 個人資料保護法第 8 條第 2 項之豁免告知事由過多，遭到學者批評，參見：張陳弘、莊植寧，前註 28，頁 219-220。

之蒐集必然造成資訊隱私權之干預，所以本來就不可能「對當事人顯無不利之影響」，且單一識別資料持續儲存於單一識別系統中，不在當事人可支配的範圍內，始終存有資訊安全的風險（且此一風險無論如何都不可能降低至零）而不利於當事人對個人資料之自主控制。更何況，若不對當事人進行告知，當事人將對上開風險欠缺完整之認識，並在此等資訊不充足的情況下作成同意之決定，無疑使得當事人資訊自主地位受損害的程度更為加劇。因此，台北市政府也不能以個人資料保護法第 8 條第 2 項第 6 款作為豁免告知義務之法律依據。既然台北市政府蒐集單一識別資料，並不具備任何豁免告知義務的事由，當然應依個人資料保護法第 8 條第 1 項之規定踐行告知義務。

(二)告知內容之明確性？

由於台北市政府在得到當事人同意而蒐集單一識別資料前，必須踐行告知義務，因此接下來必須檢視的是，台北市政府所為之告知內容是否明確。作業要點第二點（六）提到的附件一，乃是民眾申辦單一識別服務之申請表及個人資料蒐集、處理、利用同意書。在同意書中，同時列舉包括蒐集目的在內的五點告知事項。仔細閱讀同意書中的告知事項，不難發現，其告知之內容非常模糊。

1. 蒐集機關？

依據個人資料保護法第 8 條第 1 項第 1 款，行政機關向當事人蒐集個人資料，應明確告知機關之名稱。作業要點附件一同意書所載之單一識別資料蒐集機關，乃是台北市政府。然而，依據作業要點第十點，單一識別系統之統籌規劃、建置及維護機關則是台北市政府資訊局。既然人民被告知而同意的，是向「台北市政府」（而非向「台北市政府資訊局」）提供個人資料作為單一識別資料，那麼要建置單一識別系統，勢必得由台北市政府將蒐集到的資料轉交給台北市政府資訊局。由於在行政組織法上，台北市政府資訊局乃是行政程序法第 2 條第 2 項所稱具有

單獨法定地位之行政機關，而非台北市政府之內部單位⁸⁹，因此，台北市政府將蒐集到的個人資料轉交給台北市政府資訊局，並非台北市政府對個人資料之「處理」（內部傳輸）⁹⁰，而是台北市政府對個人資料之「利用」。對於台北市政府資訊局而言，其經由台北市政府轉交而取得個人資料，乃是個人資料保護法第 9 條規定之「間接蒐集個人資料」，依據個人資料保護法第 9 條第 1 項之規定，為了建置並運作單一識別系統而初次利用單一識別資料時，應踐行對當事人之告知義務。

2. 蒐集之目的？

依據個人資料保護法第 8 條第 1 項第 2 款之規定，告知內容還包括蒐集個人資料之目的。作業要點附件一同意書的告知事項一，列舉了十個蒐集目的：「交通及公共建設行政」、「社會行政」、「政令宣導」、「教育或訓練行政」、「稅務行政」、「圖書館、出版品管理」、「衛生行政」、「調查、統計與研究分析」、「學術研究」、「其他地方政府機關暨所屬機關構內部單位管理、公共事務監督、行政協助及相關業務」。

就如同實務上各機關踐行告知義務時的普遍作法一樣，以上這十個蒐集目的，全部抄自法務部（經個人資料保護法第 53 條授權）訂定的「個人資料保護法之特定目的及個人資料之類別」⁹¹。個人資料保護法第 53 條規定得很清楚，其授權法務部訂定的「個人資料保護法之特定目的及個人資料之類別」，僅供各機關

⁸⁹ 依據地方行政機關組織基準法第 5 條第 1 項第 1 款第 1 目及第 11 條第 1 項之規定，直轄市政府所屬一級「機關」定名為「局、處、委員會」，直轄市政府所屬一級「單位」定名為「處」或「委員會」。因此，台北市政府資訊局，由其組織名稱即可得知乃是行政機關，而非內部單位。

⁹⁰ 依據個人資料保護法第 2 條第 4 款之定義，機關將個人資料作內部傳輸，乃是個人資料之「處理」。因此，機關將保有之個人資料交付其他機關，並非個人資料之「處理」，而是個人資料之「利用」。就此亦可參見：詹鎮榮，前註 9，頁 9-10。

⁹¹ 就連諸如 028、057、072 此等（在法律上根本不具任何意義的）編號數字也都照抄不誤，令人感到相當困惑。

參考而已，且就蒐集目的而言，「個人資料保護法之特定目的及個人資料之類別」作為一般抽象之法規命令，只能去個案化地僅就蒐集目的之「項目」予以羅列，不可能針對每一個個案之蒐集目的予以具體規定。各機關在踐行告知義務時，若要參考法務部訂定之「個人資料保護法之特定目的及個人資料之類別」，應該要在其羅列的「蒐集目的項目」下，進一步明確具體向當事人告知其蒐集之目的究竟為何，不能照抄「個人資料保護法之特定目的及個人資料之類別」概括抽象的「蒐集目的項目」⁹²。就本文看來，作業要點附件一同意書告知事項一列舉的十個蒐集目的，都太過抽象模糊，例如「交通及公共建設行政」、「社會行政」、「教育或訓練行政」、「稅務行政」都只不過是行政事務領域的框架概念，個人資料在此等行政事務領域內的用途，有著太多的可能性，當事人根本無法藉由這樣的告知，得以清楚知悉其個人資料會被拿去作何等使用。如前所述⁹³，個人資料保護法第 15 條「公務機關蒐集個人資料，應有特定目的」的規定，同時也要求該特定目的必須正當且明確。作業要點附件一同意書告知事項一列舉的十個蒐集目的，由於太過抽象模糊，欠缺明確性，所以不符合個人資料保護法第 15 條關於「特定目的」之規定，並從而導致台北市政府一併違反個人資料保護法第 8 條第 1 項「明確告知」之要求。

此外，依據作業要點第二點（七）對於單一識別系統之定義，單一識別系統乃是「執行會員身分識別」之系統，而作業要點第二點、第三點、第十點的說明也分別指出「各服務機關為審核卡證服務及線上服務申請所需之單一識別資料，得於申請人或會員同意自單一識別系統提供」、「單一識別系統之建置目的，對各服務機關而言係用戶身分識別」、「單一識別系統之建置目的，僅在整合市政服務之用戶身分識別作業，而非將會員已取得之行政服務細節資料全數儲存於系統中，亦非供各服務機關逕行分析會員之潛在行政服務需求或從事市政行銷之用」。由

⁹² 相同的批評：劉定基，前註 46，頁 159。

⁹³ 請參見本文「參、一」。

此可見，台北市政府蒐集民眾個人資料作為單一識別資料，並據以建置單一識別系統，其目的簡單地說，在於「識別各項市政服務之用戶身分」。既然如此，令人感到困惑不解的是，為何在作業要點附件一同意書告知事項一列舉的十個蒐集目的中，會出現「政令宣導」以及「調查、統計與研究分析」這兩個蒐集目的？無論是「政令宣導」，抑或是「調查、統計與研究分析」，都和識別身分無關，何以會出現這兩個和「識別身分」無關的目的，並不清楚，而且也和前揭「非供各服務機關逕行分析會員之潛在行政服務需求或從事市政行銷之用」的作業要點訂定說明顯然自相矛盾。民眾藉由這樣的告知，無從得知其個人資料將會被哪一個機關拿去作如何的統計調查分析使用，就這一點而言，已經違反個人資料保護法對於「目的明確性」以及「告知內容明確性」的要求。再者，由於並不清楚「調查、統計與研究分析」究何所指，是否意味著台北市政府將透過單一識別系統內的資料進行（依據歐盟個人資料保護基本規章第 22 條第 1 項，當事人有權拒絕的）「個人剖析」（Profiling）⁹⁴，也十分啟人疑竇。

3. 蒐集之資料類別？

依據個人資料保護法第 8 條第 1 項第 3 款，個人資料之類別，亦屬應告知當事人之事項。作業要點附件一同意書告知事項二列舉了七種個人資料類別，也是完全照抄法務部訂定之「個人資料保護法之特定目的及個人資料之類別」，就連「個人資料保護法之特定目的及個人資料之類別」的舉例也完全抄錄⁹⁵。由於作

⁹⁴ 歐盟個人資料保護基本規章第 22 條第 1 項規定：「純粹植基於個人資料自動化處理（包含個人剖析）而作成之決定，且該決定對當事人發生法律效果或以相類方式對當事人造成顯著影響者，當事人有權拒絕之」。至於「個人剖析」，在歐盟個人資料保護基本規章第 4 條第 4 款的定義下，是指為了評價特定個人，對個人資料所為之任何形式的自動化處理。值得注意的是，有學者指出，歐盟個人資料保護基本規章第 22 條第 1 項雖然規定的是「當事人拒絕權」，但其實這一項規定也同時揭示了「包括個人剖析在內的自動化決定，原則上應予禁止」的精神，參見：*Tobias Herbst*, in: *Martin Eßer/Philipp Kramer/Kai von Lewinski (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz und Nebengesetze Kommentar*, 6. Aufl., 2018, Art. 22 DS-GVO Rn. 4.

⁹⁵ 如同前註 91 所言，被照抄的，還有諸如 C001、C003、C011 此等（在法律上完全不具任何意

業要點附件一同意書告知事項二列舉的七種個人資料類別，連「個人資料保護法之特定目的及個人資料之類別」的舉例也完全抄錄，所以其告知當事人要蒐集的個人資料類別，最後均以「例如：...」的形式結尾⁹⁶。如此一來，原本在告知項目中應屬「列舉」性質的個人資料類別，竟成了「例示」而已，導致當事人藉由該告知根本無從確定到底有哪些個人資料會被台北市政府蒐集。台北市政府蒐集單一識別資料，其對當事人所為之告知內容，除了蒐集目的不明確之外，就連蒐集的個人資料類別也不具明確性。

三、必要性？

作業要點第三點第 1 項前段之規定：「各服務機關提供之卡證服務或其為民服務之資訊系統，具有線上或臨櫃個人識別、認證或授權之功能者，應使用單一識別系統，並辦理歸戶」，第 3 項並規定：「未整合加入單一識別服務之機關服務項目，各該服務機關應與本府資訊局確認歸戶流程、期程及設計落日機制，並於官方網站公告之。服務機關若新增或停止卡證服務，應整合至單一識別系統」。在這兩項規定的要求下，台北市政府及其所屬機關的各種市政服務，其身分識別作業，未來將全部透過單一識別系統為之。民眾若要使用台北市政府及其所屬機關的各種市政服務，為了通過身分認證，必須先申請辦理單一識別服務。也就是說，作業要點第三點第 1 項以及第 3 項的規定，實質上等於強迫人民配合單一識別系統的建置而提供個人資料作為單一識別資料。

行政機關強迫人民配合單一識別系統的建置而提供個人資料作為單一識別資料，若以僅具行政規則性質的作業要點作為法律依據，如前所述⁹⁷，當然違反法律保留原則。而且，就本文看來，即便由立法者親自以法律或自治條例規定「人

義的) 編號數字。

⁹⁶ 就拿告知蒐集個人資料類別第二類來說，其所載之文字內容為：「特徵類：C011 個人描述（例如：性別、生日）」。

⁹⁷ 請參見本文「肆、一」。

民應配合單一識別系統的建置而提供個人資料作為單一識別資料」，這樣的規定恐怕也不具實質合法性。單一識別系統的建置以及單一識別服務的推行，固然是電子化政府在技術上的進步指標，但是，在法律上，人民不但沒有配合電子化政府的義務，甚至還有抗拒電子化政府的權利⁹⁸。行政機關為了要建置單一識別系統以及推行單一識別服務，實質上造成那些「不願意加入單一識別服務」、「只想透過傳統非電子數位途徑識別身分」的人民，被排拒在各種市政服務的大門之外，這恐怕已經形成不合理的差別待遇，而有牴觸憲法平等權保障的疑慮。更何況，從個人資料保護的角度觀之，建置單一識別系統以及向人民蒐集單一識別資料，對於提供市政服務而言，應該也非屬必要。如前所述⁹⁹，行政機關蒐集個人資料，應該對於執行法定職務以及特定目的之達成具有必要性，也就是說，若不蒐集該個人資料，則行政機關將無法（有效）執行其法定職務，且無法達成其欲達成之特定目的。既然各項市政服務之提供，就算沒有單一識別系統，其身分認證作業也照樣能順利進行，那麼強制人民提供個人資料作為單一識別資料並儲存在單一識別系統中，顯然並非「絕對必要」，欠缺必要性。此等不具必要性的個人資料蒐集，若非經當事人同意，實在難以取得實質合法的評價。

伍、結語

誠如李震山大法官所言，國家機關蒐集個人資料，一方面固然可藉此取得資訊作為施政之正當性基礎，另一方面卻也對人民之資訊隱私權（資訊自主決定權）造成干預，可謂具有雙面刃功能¹⁰⁰。個人資料保護法以「避免人格權受侵害，促進個人資料合理利用」之雙重立法目的，規定諸多合法性要求，為行政機關蒐集、處理、利用個人資料劃定界線，在行政機關取用個人資料之需求與個人資料自主

⁹⁸ Dirk Heckmann, Grundrecht auf IT-Abwehr? - Freiheitsrechte als Abwehrrechte gegen aufgedrängtes E-Government, MMR 2003, S. 3 ff.

⁹⁹ 請參見本文「參、五」。

¹⁰⁰ 李震山，前註 71，頁 491。

決定權之間力求折衝調和。台北市政府近來推行之單一識別系統，經本文檢視，並未符合個人資料保護法規定之各項合法性要求，除欠缺法律授權依據外，其蒐集個人資料之目的以及蒐集資料之類別，也缺乏足夠之明確性。對於單一識別系統適法性之瑕疵，台北市政府應以個人資料保護法各項合法性要求為準繩，儘速予以檢討改進，避免其對於個人資料蒐集、處理、利用之行為逾越依法行政原則之框架，更不宜高舉電子化政府之大旗，要求人民配合單一身分識別機制。