109 年臺北市柯文哲市長訪歐團

出國報告

(法務局權管部分－愛沙尼亞電子化政府相關)

壹、參訪機關簡介

參訪日期：2020 年 1 月 17 日	
參訪機關名稱	重要性
1.愛沙尼亞數位事務無任所大使、經濟暨通訊部及外交部餐敘	瞭解愛沙尼亞推動數位化政府之整體性政策。
2.愛沙尼亞 E 化政府簡報中心 (e- Estinia Briefing Center)	愛沙尼亞 ICT 展示中心，為各國了解愛沙尼亞電子化政府推動之必訪地點。
3.愛沙尼亞資訊管理局 (Information System Authority, RIA)	該機關職司愛沙尼亞全國資訊系統之發展、管理及資安維護。
4.塔林市府官邸	瞭解該市辦理電子化服務所涉之資料交換應適用法令(含歐盟及該國法令)、個人資料暨隱私權保障實務疑義及處理方式。
5.愛沙尼亞數位治理學院 (e-Governance Academy, eGA)	愛沙尼亞推動電子化政府之重要民間協力機構，研究範圍包括資訊交換、數位治理、數位民主及資訊安全。

貳、參訪過程

行程	與會人員
1.愛沙尼亞數位事務無任所大使、經濟暨通訊部及外交部餐敘	1.本府：市長、周發言人、楊執行長、資訊局 3 人、法務局 2 人、國務組吳股長、傳譯 Ando 2.愛沙尼亞：愛沙尼亞數位事務無任所大使 Amb. Tõnis Nirk；愛沙尼亞政府首席資訊長辦公室之全球事務主任 Mr. Indrek Onnik；愛沙尼亞經濟暨通訊部國家資訊系統處財務顧問 Mr. Margo Keerme；愛沙尼亞外交部亞非、拉美暨大洋洲政務司之東亞暨南亞科科員 Mr. Indrek Kiverik
2.愛沙尼亞 E 化政府簡報中心 (e- Estinia Briefing Center)	1. 本府：全團、傳譯(Ando)、地陪林怡廷、廠商代表 4 人 2. 愛沙尼亞：接待導覽人員 Ms. Anett Numa
3.愛沙尼亞資訊管理局 (Information System Authority,	本府：全團、傳譯(Ando)、地陪林怡廷、廠商代表 4 人

RIA)	
4.塔林市府官邸	1.本府：全團、傳譯(Ando)、地陪林怡廷、廠商代表 4 人 2.愛沙尼亞：塔林市政府秘書長 Mr. Toomas Sepp；塔林市政府資訊長 Mr. Martin Männil；塔林市政府資訊中心主任 Mr. Gert Väli；塔林市政府國際關係暨禮賓處處長 Ms. Heili
5.愛沙尼亞數位治理學院 (e-Governance Academy, eGA)	1. 本府：市長、5 位議員、周發言人、楊執行長、陳建璋、資訊局 3 人、法務局 2 人、3 位局長、國務組、傳譯 Ando、廠商代表 4 人 2. 愛沙尼亞：接待簡報人員 Mr. Linnar Viik

參、參訪內容

一、電子化政府推動的核心－數位身分證

(一)愛沙尼亞於 1991 年獨立初期，國土雖然不大，人口大約 130 萬人，但立國之初經費匱乏，行政服務難以觸及所有地域，因而促使執政者決心推動電子化政府，並予以立法支持。初期推動策略，是建立人口普查原則，並對每位自然人核發身分代碼(Personal Identity Code, PIC)，及一份期限 10 年的護照[1]；同時，從中小學開始推廣電腦教學，並提供年長者免費學習課程。

圖 1：與愛沙尼亞數位事務無任所大使等官員早餐餐敘

(二)配合前開護照期限將屆，愛沙尼亞政府把握時機，先於 1999 年 2 月制定「身分證法」(Identity Documents Act, IDA)，再於 2000 年 3 月制定「數位簽章法」(Digital Signatures Act)，作為數位身分證(下稱 eID)的法律基礎[2]；至 2002 年 1 月，開始正式發給民眾使用。愛沙尼亞 eID 卡證具有以下特

[1] *See* e-Governance Academy, eID Estonian experience, at 3 (December, 2013)。

[2] *Id*., at 3, 8.

色：

1、**強制持有：**依 IDA 第 5 條規定，愛沙尼亞公民均必須持有身分證；但未滿 15 歲者，得選擇持有或不持有[3]。**藉由此一強制領用身分證規定，愛沙尼亞得以迅速提高 eID 的使用率與滲透率**；相較之下，鄰國芬蘭雖提早 9 年起步，但因芬蘭並未如同愛沙尼亞以法律強制持有身分證，使得芬蘭目前仍有相當比例使用傳統紙本作業，且紙本、電子併存，亦造成受理者必須配合使用者習慣，採取多種作業配套，導致成本倍增。

2、**僅供識別：**愛沙尼亞「身分證」的法律定義，係指該國核發，記載姓名、出生日期、個人識別碼、照片及簽名影像之證明文件；類型包含實體卡證、無實體數位卡證(digital identity card，含以數位形式儲存於行動裝置之 mobile-ID[4])、護照及居留證等[5]，其中又以實體 eID 之使用率最高[6]。實體 eID 外觀設有部分可目視資訊及晶片，其中可目視資訊如姓名、出生日期、個人識別碼、性別、認證核發者與認證序號、生效及失效日期等部分，**均屬公開而不具秘密性**，實際上亦無秘密之必要，蓋此等資料在愛沙尼亞僅有初步辨識特定人功能，無從進一步接近或取得卡證持有者之公、私部門往來資料；又卡上晶片僅供上網認證使用者身分，其中不儲存任何敏感資料。

3、**結合簽章：**愛沙尼亞 eID 不論為實體或數位形式，**均同時具備「身分驗證」及「電子簽章」2 種功能**[7]。單純進行身分驗證時，使用者須輸入 4 位數密碼；使用電子簽章時，則輸入 5 位數密碼。

4、**法定效期：**愛沙尼亞 eID 不論為實體或數位形式，依法有效期限均為 5 年[8]；護照之效期則為 10 年[9]。

(三)截至目前，愛沙尼亞累計有 7 億次數位簽章、95%以上納稅義務人使用數位方式報稅、一半投票權人使用電子投票，及 96%病患使用電子處方箋，顯示對電子系統的高度依賴，亦凸顯資通安全的重要性。愛沙尼亞的資通安全維護，主要由該國資訊管理局負責統籌，包括定期舉辦全國性的資通研討會，進行公、私部門交流，及資安宣導規劃(例如：透過地方性圖書館館員，接觸高齡者，加強資安知識宣導)。

---

[3] *See* IDA §5: (1) An Estonian citizen residing in Estonia shall hold an identity card. (2) An Estonian citizen specified in subsection (1) of this section who is under 15 years of age need not hold an identity card.

[4] *See* IDA §20[4] (1).

[5] *See* IDA §2 (1), (2).

[6] *See* Republic of Estonia Information System Authority, Means of eID，https://www.ria.ee/en/state-information-system/electronic-identity-eid/means-eid.html; last visited：2020.2.22。

[7] *See* IDA §§9[4](1), 19[1] (1), 20[2] (1).

[8] *See* IDA §§20(1), 20[3].

[9] *See* IDA §24(1).

圖 2：愛沙尼亞Ｅ化政府簡報中心簡介 eID

二、電子化政府技術骨幹－X-Road

(一)X-Road 愛沙尼亞中央政府開發的開源數據交換解決方案，使各公、私部門可以藉由網路交換資料，主要功能包括：控管網址、資訊發送與訪問權限；對傳輸各方進行組織與設備等級認證；執行傳輸加密、數位簽章；加註時間戳記，及進行錯誤管理等[10]。該方案作為愛沙尼亞全國性的資料傳輸平台，屬於該國「公眾資訊法」(Public Information Act, PIA)第 43 條之 9 第 1 項第 5 款所定應由中央政府立法維運之國家級資訊系統[11]。

(二)X-Road 的開源特性，使得公、私營部門均可將其資訊系統與 X-Road 相連，或使用相容架構建置部門內部系統，以節省資源，進一步提升公部門間、私部門間及公、私部門間的數據交換效率。又對於民眾及消費者而言，透過 X-Road 能夠穿梭不同網路門戶，使用各種服務，同時掌握自己在各公、私部門之資料運用情形[12]。

[10] *See* X-Road, X-ROAD INTRODUCTION, https://x-road.global/; last visited：2020.2.22。

[11] *See* PIA §43[9]: "(1) The following support systems for the maintenance of databases shall be established by a Regulation of the Government of the Republic: …5) the data exchange layer of information systems; …".

[12] *See* e-Governance Academy, eID Estonian experience, at 13-14 (December, 2013)。

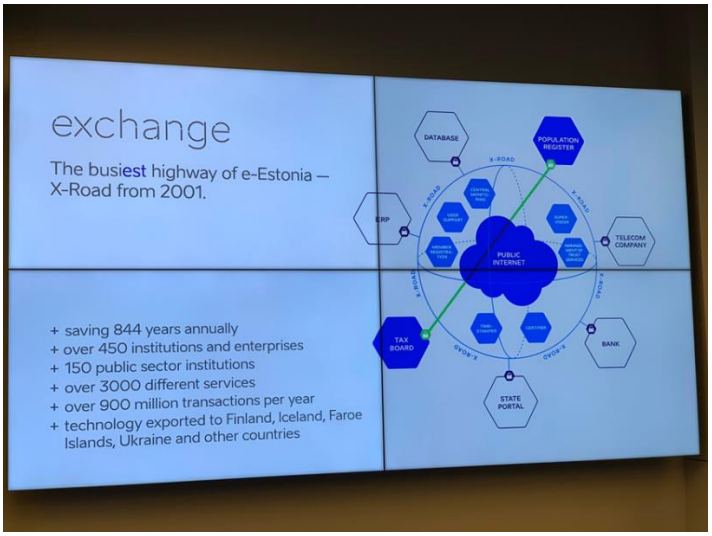

圖 3：愛沙尼亞資訊管理局簡報 X-Road 運作架構

三、電子化政府之法令遵循及重要作業原則

(一)愛沙尼亞的電子化政府實踐，立基於成千上萬的個人資料蒐用與流通，因此在 eID 及 X-Road 以外，**法令遵循亦被該國視為電子化政府的支柱**。作為歐盟會員國，愛沙尼亞自 2018 年 5 月 25 日開始，須適用號稱史上最嚴格個人資料保護規範之「歐盟一般資料保護規範」(General Data Protection Regulation, GDPR)；關於 GDPR 施行後對愛沙尼亞推動電子化政府及個人資料交換的影響，塔林市資訊長 Martin Männi 表示：在該市行政實務上，涉及市民個人資料蒐用之行政行為，**均已有相對應之法律規定**。是以，**該市無須個別取得資料當事人之同意，得逕依相關內國法律規定蒐用個人資料、執行行政任務**，與 GDPR 並無違背，法令亦無大幅修正需求，但可能須配合調整資訊系統運作方式[13]。

(二)其次，因 GDPR 第 12 條第 1 項規定，明文要求資料管控者應採用簡明易懂且方便取得之格式，對資料當事人告知蒐用之特定目的等相關訊息[14]，愛沙尼亞對此有何特殊作法？Martin Männi 回應：因蒐用前必須告知之事項，均由 GDPR 等法律所明定，塔林市目前並未採取較傳統不同的方式進行告知。

(三)作為愛沙尼亞首都，塔林市政府目前有 60 個線上行政服務系統，提供 1 百餘種行政服務項目；除了使用全國通用的基礎系統，也會配合市民的特殊需求，較中央政府更早開發相應的線上服務(例如：透過市民線上交換目擊訊息，協尋寵物)。而在開發新系統或服務前，塔林市政府會先將市民進行

[13] 此所謂資訊系統運作方式之調整，似指 GDPR 第 22 條第 1 項新定之「限制個人自動化決策權」；亦即，當公、私部門單純運用電腦或機器對個人資料採取自動化分析，進而對資料當事人產生無從預見之重大影響，甚至有所歧視之分類效果時，GDPR 賦予當事人拒絕此種分析方式之權利。相關說明，參閱：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 6 月，頁 208-214。

[14] 同前註，頁 177-178。

各種分類(例如：年齡、行為模式、是否為身心障礙等)，進行需求分析，及各類群體接收訊息之方式；同時，為落實依法行政、確保政府資訊透明及系統發展平衡，開發前須查詢愛沙尼亞資訊管理局建置之「RIHA」(Riigi Infosüsteemi Halduse Infosüsteem)系統[15]，**確認規劃中之系統或服務，可能涉及之個人資料種類、位於那些資訊系統及相對應之法律依據**。

(四)愛沙尼亞政府在蒐用民眾個人資料時，尚遵守「一次蒐集」及「公開透明」兩大原則；

1、「一次蒐集」係指：**一筆或一項個人資料，僅由單一蒐用機關保有[16]；同一民眾至其他機關申辦業務所提供之資料，亦由該他機關單獨保有**；如對於留存於他機關之資料有需求，則透過 X-Road 系統流通取得。其背後原理為：避免單一機關對個別民眾擁有絕對優勢的資訊量，降低資訊集中之可能風險，同時減少不同機關重複蒐集相同資料之繁瑣。

2、其次，所謂「公開透明」係對於卡證資料當事人而言，**其得隨時登入系統查閱卡證資料被各類公、私部門查詢及利用之軌跡**。在 X-Road 機制下，除了原保有之公務或非公務機關外，透過系統交換取得資料者，僅能短暫接觸該筆資料；一旦需用業務辦理完成，該筆資料隨即自取用者電腦或網路上消失，防止不當之留存。例如：塔林市民享有搭乘該市公車免費之優惠，惟是否具備市民資格，有待公車業者透過 X-Road 交換住址資料進行比對；此項資料比對之軌跡，得由乘客登入系統查知，確保其個人資料蒐用為當事人本人可知及管理；又如發現確有不當蒐用行為，資料當事人得逕洽蒐用者了解原因，或請求個人資料保護專責機關查處。

四、其他具特色之電子化政府案例

(一)塔林市政府目前已將府內各種會議資料，於開會前 24 小時放置於雲端，供與會者及外界參考。不過，這種作法有時會造成外界過度解讀，誤認尚未拍板之議題為既定政策。

(二)人民線上申請使用公共場域舉辦活動時，申請系統將自動通知塔林市政府所有相關機關，並自動彙整與個案場地相關之資訊，回報申請人特定時段是否可用、有無施工等，避免各機關因人工橫向聯繫不足而誤為准駁，或漏未提醒申請人重要事項。

---

[15] 「RIHA」是愛沙尼亞全國性的「資訊系統目錄」，由愛沙尼亞資訊管理局維運；其內容包括各系統蒐用那些資訊、各系統之管理者、聯絡方式、運作之法律基礎、各系統間協作所需之共用程式碼及組件。*See* Republic of Estonia Information System Authority, Administration system for the state information system RIHA, https://www.ria.ee/en/state-information-system/administration-system-riha.html; last visited：2020.2.22。

[16] 關於「一次蒐集」原則之具體法律依據，例如：PIA 第 43 條之 3 第 2 項規定，明文禁止針對同一資料建置不同之資料庫加以蒐用。*See* PIA §43^3(2): Establishment of separate databases for the collection of the same data is prohibited.

肆、參訪心得

一、愛沙尼亞與本府推動電子化政府之整體法律規範架構比較

(一)愛沙尼亞：

1、觀諸 2019 年歐盟電子化政府推動概況(Digital Government Factsheet 2019 Estonia)對於愛沙尼亞整體法規架構的描述，愛沙尼亞迄今並無制(訂)定電子化政府的專門法規，而是按電子化政府運作將涉及的各個領域，分散規定其行為及作用事項。例如：電子化政府必須使民眾及參與之公、私部門得以自由接觸公開資訊，在此領域，即有前述 PIA 及「檔案法」(Archives Act)作為依據；在 eID 領域，有 IDA 規範國民持有身分證之義務、eID 得承載之個人資料[17]及 eID 之功能等；在資訊安全與個人隱私保護領域，有「數位安全法」(Cybersecurity Act)及個人資料保護法(Personal Data Protection Act[18], PDPA)[19]。

2、此外，在愛沙尼亞個別行政任務法律中，亦可散見電子化相關規範。例如：關於人口登記資料維護，該國「戶籍法」(Population Register Act, PRA)，第 8 條明定應以電子資料庫形式為之，相關資料亦得依法為線上或自動化處理[20]；「土地登記法」(Land Register Act, LRA)定有線上土地登記專章[21]，除適用土地登記之一般規定外[22]，並明定線上資料處理之應行事項[23]及電子簽章使用情境[24]；又該國「公司法」(Commercial Code, CC)除定有線上申請相關規定外[25]，第 67 條第 1 項並明定商業登記資料應以電子方式保存[26]。

3、值得注意的是，雖然電子化政府運作績效斐然，愛沙尼亞並未在法律中全面性地強制民眾必須接受及使用線上作業。依該國「行政程序法」(Administrative Procedure Act, APA)第 5 條第 1 項及第 2 項規定，除其他法規另有明文外，**行政機關應依職權裁量行政程序行為暨各類細部作業「所採取之形式」**，且行政程序應合於目的，兼具效率、直接，避免不當

---

[17] 除姓名、出生年月日、個人識別碼、性別、公民資格與簽名影像外，亦得納入其他生物辨識資料，包括指紋影像、虹膜影像及髮色等。*See* IDA §9(3).

[18] 在歐盟 GDPR 生效後，因直接產生各會員國之內國法效力，故 PDPA 之定位轉變為 GDPR 在愛沙尼亞之補充與執行規範，同時作為個人刑事犯罪資訊交換、個人資料處理過程之遵法監督，及違法處理個人資料之究責等依據。*See* PDPA §1.

[19] *See* Digital Government Factsheet 2019 Estonia, at 10-15.

[20] *See* PRA §8: "(1) The population register is maintained as an electronic database. (2) Automatic data processing is used upon the processing of data in the population register. (3) Data in the population register may be processed online under the conditions and pursuant to the procedure provided for in this Act…".

[21] *See* LRA Chapter 10^1 ELECTRONIC LAND REGISTER.

[22] *See* LRA §77^1(2).

[23] *See* LRA §77^3.

[24] *See* LRA §77^8.

[25] *e.g.* CC §33.

[26] *See* CC §67(1): The commercial register shall be maintained using electronic means.

稽延、耗費過多成本或造成民眾不便[27]；同法第 14 條第 1 項規定，**申請人得任擇其申請形式**，並於送達行政機關後，開啟行政程序[28]，第 2 項至第 4 項則就口頭、書面(應記載事項)及電子申請(須電子簽章加簽，必要時並採取電子封緘)加以規定[29]。此外，行政程序中相關文書之送達，亦維持郵寄、電子方式併行[30]。

(二)我國及本府：在電子化政府推動方面，我國或本府目前尚無整合性的立法，與前述愛沙尼亞法制架構相近－電子化行政作業之規定，散見於各部門主管之法規。就中央立法、本府作為主管機關之重要法律而言，大致有以下幾類電子化作業規定：

1、以電子文件方式送達。例如：行政程序法第 68 條第 2 項、公司法第 28 條之 1 第 1 項。

2、以電子文件方式儲存。例如：檔案法第 12 條第 3 項規定，經檔案中央主管機關核准銷毀之檔案，必要時，應先經電子儲存，始得銷毀。

3、以電子文件方式申請，並結合電子簽章。例如：政府資訊公開法第 10 條第 2 項規定，申請提供政府資訊之申請書，得以書面通訊方式為之；其申請經電子簽章憑證機構認證後，得以電子傳遞方式為之。又例如：戶籍法第 28 條規定，以網路申請戶籍登記時，應以電子簽章為之，且該電子簽章限以自然人憑證為之。此外，土地登記規則第 36 條，亦規定以網路申請登記者，相關電子文件應以電子簽章方式辦理。

(三)小結：對比愛沙尼亞與我國及本府之電子化政府法制架構，目前均無單一專法或自治法規加以規範。在此基礎下，因缺乏單一權責機關進行整體規劃及業務協調，各機關經年累月的作業積習，易導致電子化作業及資料庫管理均各自為政。**然而，愛沙尼亞推動電子化政府之成效，似乎未受法制架構分散所影響；透過本次參訪可以發現，強制性的 eID 卡證持有，及整合各個公、私部門的統一資料交換系統 X-Road，應為箇中關鍵**。

二、愛沙尼亞與本府身分識別機制之差異

(一)愛沙尼亞 eID：

---

[27] *See* APA §5(1) An administrative authority **shall determine the form** of procedural acts and other details of administrative procedure **on the basis of the right of discretion** unless otherwise provided by an Act or regulation. (2) Administrative procedure shall be purposeful, efficient and straightforward and conducted without undue delay, avoiding superfluous costs and inconveniences to persons.

[28] *See* APA §14(1): " A request (application) in a freely chosen form shall be submitted to an administrative authority for the commencement of administrative proceedings, or in the course of administrative proceedings…".

[29] *See* APA §14: "(2) An administrative authority shall take minutes of oral applications. (3) A written application shall set out the following:…. (4) A digital signature and, if necessary, an electronic seal shall be added to an electronically transmitted application. A digital signature and electronic seal need not be added, if the application has been submitted by an electronic channel, and the administrative authority has identified the applicant in a secure manner."

[30] *See* APA §25 (1): Administrative acts, summonses, notices and other documents shall be served on the participants in proceedings either by post, by the administrative authority which issued the document or by electronic means.

1、在愛沙尼亞 eID 的官網簡介中，有以下這段敘述：「Unlike in many other countries, every Estonian, irrespective of their location, has a state issued digital identity.[31]」顯然有意藉此表彰身分證的獨特性及凸顯 eID 在電子化政府的地位。這對於已習於隨身攜帶並妥善保管身分證的我國國民或本市市民來說，實在談不上有何新穎；真正顛覆吾人想像的，是該國 eID 的廣泛用途及背後原理。

2、如前所述，愛沙尼亞 eID 不分實體或數位形式，均具有「僅供識別」及「電子簽章」之特點，顯示該國對於「識別」一詞賦予更為實用性的義涵；亦即，在一般用以辨識特定個人的資料之外，同時將申請、交易實務上經常使用的簽章列入 eID 中。**就使用者之角度而言，此種實用義涵的加入，係提供持用身分證的積極誘因，而不僅是消極履行 IDA 之法定義務。**在此基礎上，配合「一次蒐集」之簡便性、「公開透明」的軌跡查詢機制、X-Road 的全面資料交換機制，以及該國立國以來的政策堅持，使得 eID 在該國可以深入國民的日常生活，成為不可或缺的一部，建立深刻的忠誠度與依賴性。

(二)本府「臺北通」：

1、為推動電子化政府，整併、統一市民各項服務申請之身分識別機制，本府前於 108 年 9 月 20 日訂定發布「臺北市政府單一識別服務作業要點」(下稱本府單一識別要點)，作為「臺北通」系統的法令依據。其身分識別機制之運作，係透過蒐集或歸戶申請人姓名、身分證字號、性別、出生年月日、電話(手機)號碼、電子信箱及戶籍地址等個人資料，給予申請人單一數位身分，亦即帳號及密碼組成之金鑰，供其線上或臨櫃申請本府所屬各機關(構)或學校服務時「識別身分」之用(詳本府單一識別要點第 2 點第 4 款、第 8 款及第 3 點第 1 項規定)。同時，為使民眾能夠一目瞭然其已開通及未開通之卡證服務項目，單一識別系統亦統整各機關(構)之卡證服務資訊並予以個別註記(詳本府單一識別要點第 2 點第 5 款規定)。至於個案行政服務之提供，將於身分識別完成後，另由民眾依相關法令洽各機關申辦，而非由單一識別系統直接提供；是以，單一識別系統除上述身分識別及卡證服務註記外，並不蒐集、處理或利用其他行政服務細部資料，亦非各機關(構)或學校交互流用個人資料之管道(詳本府單一識別要點第 10 點第 1 項第 3 款規定)。

2、相較於愛沙尼亞 eID，臺北通之主要特色包括：第一，屬於**完全數位化卡證**，並無 eID 實體、數位併存之情形；第二，僅具有身分識別之金鑰功能，**並未結合數位簽章**，亦無明確之數位簽章使用情境；第三，單純作為使用者身分識別，**不提供資料交換使用**；第四，配合本府所屬各機關過去自建身分辨識機制之現實，**需強制改用臺北通並設定歸戶機制**，始能發揮統一身分識別之機能；第五，**法令基礎僅為行政規則**，屬於現行

[31] *See* e-estonia, e-identity, https://e-estonia.com/solutions/e-identity/id-card/; last visited：2020.2.24。

法制體系下位階偏低之規範。

3、誠然，本府運作早於愛沙尼亞獨立時間，因傳統之行政機關權責劃分，與過去對於個人資料之價值、隱私權保障尚無明確意識，進而形塑出所屬機關個別之身分識別機制及公務資料庫；其無從比照愛沙尼亞採取個人資料之「一次蒐集」原則，當無可厚非。惟在不具備電子簽章及其他加值運用之前提下，強制市民在取得線上或臨櫃服務前，須一律採行臺北通之線上身分辨識，**可能違背其熟悉之使用習慣，或缺乏改變習慣之誘因，甚至有不當限制其權利行使之疑慮**。此外，因臺北通僅以行政規則為其辦理依據，如遇中央法規、本府自治條例或自治規則有不同規定時，**執行面易生法遵風險**。

三、愛沙尼亞與本府個人資料保護法制

(一)愛沙尼亞：因屬歐盟會員國，愛沙尼亞目前存在兩部主要個人資料保護規範：一為 GDPR，另一為愛沙尼亞制定之 PDPA。其中，GDPR 之規範特色包括：

1、對於「個人資料」採取從寬認定，只要資料內容、目的有關於特定個人，或使用結果可能對特定個人之權益產生影響，皆屬個人資料之範疇[32]。

2、基於個人資料蒐用行為之透明性要求，**蒐用前應以簡明易懂之語言與便利之方式**，使資料當事人知悉資料管控者、蒐用目的及日後使用方式等資訊[33]。

3、不區分蒐用行為人為公務機關或非公務機關，均適用相同之蒐用合法要件。具體而言，取得「資料當事人同意」者，當屬合法之蒐用行為，惟 GDPR 強調該同意必須符合「出於自由意志」、「受充分告知」及「具體」等要件；**在政府機關蒐用之情形，因對於一般民眾處於優勢地位，須確認個案中雙方不對稱之權力關係已經消除，始屬「出於自由意志」之同意**[34]。又如政府機關係因「履踐公共任務」所為蒐用，應同時符合「必要性」之要件，**不得僅以(可能)使公共任務之執行更為便利，或有助於抽象之公共利益為其依據**[35]。

4、逾越原蒐用目的之後續資料利用行為，除取得資料主體之同意，或依各會員國內國法律屬必要且依適當方式所為者外，原則上應審酌：前、後目的之關聯性、當事人得否合理預期、資料敏感程度、目的外利用所生影響，及有無採取適當加密或假名化措施等，確認具有「相容性」時，始屬適法[36]。**但基於科學、歷史或統計目的所為者，則視為與原蒐用目的**

---

[32] 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 6 月，頁 22-23。

[33] 同前註，頁 178。

[34] 同前註，頁 87-89。

[35] 同前註，頁 97。

[36] 同前註，頁 127-129。

相符[37]。

5、資料當事人得主張「限制自動化決策權」，亦即當其資料被用於機器處理，並由機器獨自衡量其特徵、面向，進而加以歸類或評等時，因該等決策缺乏人工介入，可能嚴重影響當事人之權益、導致排斥或歧視，故賦予當事人拒絕權[38]。

至於目前僅具 GDPR 補充功能的 PDPA，亦有以下特色規範；

1、基於學術、歷史或政府統計之需求，得將個人資料予以假名化或採取相當之保護措施後，不經當事人同意即予以處理[39]；**行政機關基於行政目的所為分析、研究，視同該法所定學術研究**。在此範圍內，行政機關有權查詢或利用其他控制者或處理者之資料庫，但應先取得愛沙尼亞個人資料保護專責機關，即「個人資料保護檢查團」(The Estonian Data Protection Inspectorate)之許可[40]。

2、明定個人資料蒐集、處理或利用之一般原則(前述專責機關得豁免適用[41])，包括：公平、合法、特定目的須具體明確、適當、不得逾越特定目的、應以特定目的達成時為資料保存期限，及應確保資料安全等[42]。其中，資料保存期限應遵守歐盟或愛沙尼亞法律規定；如無特別規定，資料保有者應自行建立期限[43]。又特定目的外之個人資料處理，僅於歐盟或愛沙尼亞法律有規定者，或為履行此等法律所定義務者，始屬合法[44]。

3、特種(敏感)個人資料之處理，應限於絕對必要，且須有法律明文准許，為保護當事人之重大利益或該等資料已明顯公開者，始得為之[45]。如基於學術、歷史需要而處理此類個人資料，尚須先行取得相關領域之倫理委員會許可；無對應之倫理委員會者，則應取得專責機關許可[46]。

(二)本府：目前我國全國各公務機關，均適用中央制定公布之個人資料保護法(下稱個資法)。該法 2010 年全盤修正之內容，脈絡可溯自 1995 年「歐盟資

---

[37] 同前註，頁 128。

[38] 同前註，頁 208-209。

[39] *See* PDPA §6: "(1) Personal data may be processed without the consent of the data subject for the needs of scientific and historical research and official statistic, in particular in a pseudonymised format or a format which provide sequivalent level of protection…".

[40] *See* PDPA §6 (5): For the purposes of this Act, **scientific research is deemed to also include any analyses and studies by executive power which are carried out for the purposes of policy development.** In order to prepare these, the executive power has the rights to make queries to databases of another controller or processor and process the personal data received. The Estonian Data Protection Inspectorate shall verify, prior to the beginning of the specified processing of personal data, compliance with the terms and conditions provided for in this section, except in the case the objectives of the studies conducted for policy development and the scope of processing of personal data derive from legislation.

[41] *See* PDPA §12 (2).

[42] *See* PDPA §14.

[43] *See* PDPA §17 (1).

[44] *See* PDPA §16 (1).

[45] *See* PDPA §20 (1).

[46] *See* PDPA §6 (4).

料保護指令」，惟相較於 GDPR 已有相當落差。整體規範架構，除明定個人資料種類(直接/間接識別、一般性/敏感性)、蒐用行為之比例原則、特定目的拘束原則(原則上禁止特定目的外之利用行為)、資料當事人之權利、蒐用者對當事人之告知義務等事項，並區分「公務機關」與「非公務機關」，為兩者設計不同之資料蒐集、處理或利用行為要件，及違法究責機制。

(三)小結：

1、在數位網路時代，不論是電子化政府之推動，或私人企業之精準行銷，均需大量蒐用個人資料及數據，諸如歐盟 GDPR、愛沙尼亞 PDPA 及我國個資法等相關法規即應運而生，藉以確保資料當事人知的權利，並使隱私風險合理、可控。實則，資料蒐用者與資料當事人間之利害關係，係持續拉鋸，而非全有或全無之零和狀態，相關法令規定亦須在「保護不足」與「過度禁止」間審慎衡酌；我國個資法第 1 條即揭明：**「避免人格權受侵害」及「促進個人資料之合理利用」**，皆為該法立法目的。惟因此等特質使然，**個人資料保護法令經常出現原則與大量例外並立之情形；在實務執行上，亦無法如同一般刑事案件般，明確獲致犯罪是否成立之結論，而須藉由比例原則之操作，充分論述個案之利弊得失**。

2、鑒於 GDPR 以嚴格聞名，本次參訪乃特別詢問塔林市政府資訊長該法所造成之影響；其回應內容與前述 GDPR 規定以「資料當事人同意」為原則之架構是否相符，固有待研究，惟如係將愛沙尼亞內國法律所定電子化政府相關法律規定，均解為「履踐公共任務所必要」，應無違悖 GDPR 之疑慮。此等法令解釋適用方式，對本府推動電子化政府亦有重要啟發：**作為歐盟會員國，愛沙尼亞遵守 GDPR，如同本府面對中央所定個資法一般；本府如能制定自治條例，在未牴觸個資法之前提下，似可於其中配合實務需求，明定排除個資法適用之規定**。

3、揆諸實際，上開啟發與個資法規定，並無不符。按個資法第 15 條第 1 項第 1 款規定：「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：一、執行法定職務必要範圍內。」復依個資法施行細則第 10 條第 2 款及第 3 款規定，所謂「法定職務」，包括「自治條例」或「自治條例授權之自治規則」所定者。**是就個人資料之特定目的內利用行為而言，目前已得透過自治條例制定合法蒐用之依據；日後如中央有修正個資法之規劃，爭取以自治條例作為豁免告知義務及特定目的外利用之合法事由，亦為可努力之方向**。

4、另外，關於蒐用個資前履行告知義務之方式，GDPR 雖規定應以簡明易懂之文字為之，惟本次參訪自塔林市政府資訊長獲得之回應，似乎仍維持一般常見之告知內容，亦即在告知文件上臚列所有法定應告知之事項。此種困境在我國公務機關與非公務機關亦十分常見，蓋個資法第 6 條第 2 項、第 8 條及第 9 條既明定蒐集、處理個人資料前應告知之事項，「依法律規定」撰寫告知內容及可能之特定目的類型，本無違法可言；問題

在於，此種告知模式，資料當事人往往無暇細閱或充分了解其內容，縱使形式上已履行法定義務或徵得其同意，亦暗藏法遵風險，衍生「無實益告知、同意」之疑慮[47]。對此，本府日後如擴大臺北通之功能並提升其規範位階至自治條例，似可參考愛沙尼亞 eID 所遵循的「公開透明」原則，**在法定告知義務外，明文賦予資料當事人得隨時追蹤蒐用軌跡之權利，作為個資法第 3 條第 1 款與第 10 條所定查詢權之實務配套，體現對其資料自主權之尊重，同時強化對於臺北通系統之信賴及使用意願**。

伍、參訪建議

臺北通作為本府推動電子化政府之重要機制，藉由本次參訪所獲愛沙尼亞相關法律及實務運作訊息，茲提出以下法制面相關建議：

(一)提升臺北通之法源依據，至自治條例位階，並配合本府未來推動電子化政府之藍圖，在不牴觸個資法等其他上位階法規之前提下，儘量完備其作業規範內容，例如擴大個人資料之蒐用合法事由或其他個資法之特別規定，使所屬機關有推動電子化政策之堅實基礎。

(二)推動臺北通時，是否不分過去既有卡證使用情形，一律強迫歸戶，宜於研訂自治條例時充分審酌其利弊。如維持現行歸戶原則，為增加市民使用臺北通之意願，可考慮在現有身分辨識功能以外，擴充其他應用情境，及配合實際需求，加入電子簽章功能；同時，宜採行類似愛沙尼亞 eID 之蒐用軌跡追蹤機制，並加強安全性宣導，俾減少使用者疑慮。

(三)鑒於個人資料保護法令具有高度之利益權衡屬性，不論日後個資法及本府單一識別要點有無修正，本府類一條鞭法制人員，允宜強化相關知能，俾適時指導所屬機關於蒐用個人資料前，應分析、衡酌那些因素及利害關係，落實比例原則於實際施政過程，促進個人資料在公務上之合理使用。

[47] 我國學者亦有類似觀察，參閱劉定基，大數據與物聯網時代的個人資料自主權，憲政時代第 42 卷第 3 期，2017 年 1 月，頁 275-277。