

台灣經濟論衡

Focus

歐盟GDPR簡介與我國政府因應推動方向

Report

政府與產業因應 GDPR 之調適措施
GDPR 之國際傳輸

Viewpoint

GDPR 與數位經濟——歐盟的企圖與啓發
GDPR 與我國個人資料保護法之比較分析

Special Report

區塊鏈國際趨勢
臺中市畢業證書區塊鏈應用案例

歐盟 GDPR 已於今年 5 月 25 日全面施行，引起各國高度關注。面對號稱史上最嚴格的 GDPR，政府將全面協助企業因應。同時為補足我國目前個資保護採取的分散式管理機制所缺乏的協調與整合功能，政府亦已成立「個人資料保護專案辦公室」，以統籌各部會辦理 GDPR 因應相關事宜，並將持續與歐盟洽談國際傳輸適足性認定。



台灣經濟論衡

Taiwan Economic Forum

Since 1954 原《自由中國之工業》formerly *Industry of Free China*

發行人 陳美伶
副發行人 鄭貞茂、曾旭正、高仙桂
發行所 國家發展委員會
地址 10020臺北市中正區寶慶路3號
No. 3, Baoqing Rd., Zhongzheng Dist., Taipei City 10020 Taiwan (R.O.C.)
電話 (02)2316-5838 謝學如
網址 www.ndc.gov.tw
編輯所 左右設計股份有限公司
查詢專線 (02)2781-0111 分機 204 張欣宇
Email: TEF@randl.com.tw

為將期刊推廣至更多民眾，同時因應環保考量，《台灣經濟論衡》自2016年第1季起，逐步以電子書取代紙本寄贈。季刊內容可至國發會網站（www.ndc.gov.tw）首頁下方快速連結區（「台灣經濟論衡」banner）下載。如您有紙本需求，請至政府出版品集中展售中心購買。

To disseminate the publication to a wider readership and to protect the environment, since the 1st quarter of 2016 we have been gradually reducing the printing copies of the Taiwan Economic Forum.

Readers are advised to download the E-books of this publication from the website at (www.ndc.gov.tw). Meanwhile, paper copies of the publication might be available for purchase at some designated locations as follows: Wunan Bookstore (Zhongshan Rd. in Taichung), Sanmin Bookstore (Chongqing S. Rd. in Taipei), or Government Publications Bookstore (Songjiang Rd. in Taipei).

政府出版品集中展售中心

臺中五南文化廣場 (www.wunanbooks.com.tw)
TEL: (04)2226-0330 | FAX: (04)2225-8234
40042臺中市區中山路6號
No. 6, Zhongshan Rd., Central Dist., Taichung
City 40042, Taiwan (R.O.C.)

三民書局 (www.sanmin.com.tw)
TEL: (02)2361-7511 | FAX: (02) 2361-3355
10045臺北市重慶南路1段61號
No. 61, Sec. 1, Chongqing S. Rd., Zhongzheng
Dist., Taipei City 10045, Taiwan (R.O.C.)

國家書店松江門市
(國家網路書店www.govbooks.com.tw)
TEL: (02)2518-0207 | FAX: (02)2518-0778
10485臺北市中山區松江路209號1樓
1F., No. 209, Songjiang Rd., Zhongshan Dist.,
Taipei City 10485, Taiwan (R.O.C.)

中華郵政台北誌字第12號 執照登記為雜誌交寄
ISSN 1727-8627
GPN 2010300195

因應歐盟GDPR 兼顧數位經濟發展與個人資料保護

隨著數位科技與全球化的快速發展，網路安全與保護個人資料議題已儼然成為數位經濟發展的重大挑戰。為提升個人資料保護規範密度，並建立歐盟境內一體適用之管理規範，歐盟於 2016 年 5 月 24 日通過「一般資料保護規則」(General Data Protection Regulation, GDPR)，並自今(2018)年 5 月 25 日全面施行。由於歐盟此套嚴格的個人資料保護法制架構，因適用範圍可能擴及歐盟境外企業，已經引起各國的高度關注，並積極研擬政策妥為因應。

為使讀者深入瞭解歐盟 GDPR 架構之內容及影響，本期「政策焦點」特別專載「歐盟 GDPR 簡介與我國政府因應推動方向」一文，簡介 GDPR 的重要規範(包括加重企業責任、強化當事人權利、個人資料國際傳輸、提高罰則金額等)，以及我國政府的因應對策(包括成立「個人資料保護專案辦公室」、與歐盟洽談適足性認定事宜、舉辦研討會及宣導說明會等)；另在「專題報導」則刊載「政府與產業因應 GDPR 之調適措施」、「GDPR 之國際傳輸」等專文，分就政府及企業如何調適及因應 GDPR 個人資料跨境傳輸規範進行說明。

「名家觀點」單元則邀請兩位專家提供精闢見解，其中理律法律事務所曾更瑩律師在「GDPR 與數位經濟——歐盟的企圖與啟發」一文，闡述歐盟在個人資料保護與數位經濟發展之間如何調適與平衡；另國發會法制協調中心李世德參事的「GDPR 與我國個人資料保護法之比較分析」一文，則以 GDPR 體系重要架構與我國個人資料保護法進行比較分析，瞭解其中異同之處。此外，自本季開始，本刊取消「經濟統計」單元，新增「特別企劃」單元，簡述與當期主題相關、且具未來性、前瞻性之政策議題，本期即與讀者分享「區塊鏈」國際目前發展趨勢以及在臺灣的應用案例。

最後，本期「國發動態」單元報導 2050 國土空間發展願景、出席 APEC 經濟委員會第 2 次會議(EC2)暨結構改革高階官員會議、2018 年景氣指標及對策信號檢討與修正說明、中華民國人口推估(2018 至 2065 年)等本會最新動態，期有助於讀者掌握國發會業務的最新進展。

目錄

中華民國107年9月
第16卷第3期
Volume 16, Number 3
SEP. 2018



政策焦點 Focus

- 04** 歐盟 GDPR 簡介與我國政府因應推動方向
國家發展委員會



專題報導 Report

- 15** 政府與產業因應 GDPR 之調適措施
資訊工業策進會科技法律研究所 戴豪君、林其樺
- 30** GDPR 之國際傳輸
國發會法制協調中心



名家觀點 Viewpoint

- 49** GDPR 與數位經濟——歐盟的企圖與啟發
理律法律事務所 曾更瑩律師
- 69** GDPR 與我國個人資料保護法之比較分析
國發會法制協調中心參事 李世德



特別企劃 Special Report

- 94** 區塊鏈國際趨勢
國發會綜合規劃處
- 106** 臺中市畢業證書區塊鏈應用案例
臺中市政府資訊長 蕭景燈 / 臺中市西區大同國小教師 蕭聖哲



國發動態 Development

- 115** 青年世代領航，描繪 2050 國土空間發展願景
國發會國土區域離島發展處
- 119** 出席APEC經濟委員會第2次會議(EC2)
暨結構改革高階官員會議
國發會綜合規劃處
- 126** 2018 年 APEC 企業諮詢委員會 (ABAC) 數位創新論壇 (DIF)
國發會綜合規劃處
- 131** 臺灣新創勇闖 2018 香港 RISE，再傳捷報
國發會產業發展處
- 136** 2018 年景氣指標及對策信號檢討與修正說明
國發會經濟發展處
- 142** 中華民國人口推估 (2018 至 2065 年)
國發會人力發展處
- 146** 歐盟一般資料保護規則 (GDPR) 研討會
國發會法制協調中心



政策 焦點

FOCUS

歐盟GDPR簡介與我國政府因應推動方向

國家發展委員會

壹、前言

貳、歐盟 GDPR 簡介

參、我國政府因應推動方向

肆、結語

壹、前言

數位經濟時代下，大數據流通與資源分享已是不可逆的趨勢，如何讓個人資料的運用發揮價值，並兼顧隱私保護，便成為重要的課題。歐盟為了讓個人資料的保護規範因應時代變遷，並建立一體適用的管理規範，在 2016 年通過一般資料保護規則（General Data Protection Regulation, GDPR），並於今（2018）年 5 月 25 日全面施行，GDPR 建立了一套嚴格的個人資料保護法制架構，適用範圍更可能擴及歐盟境外的企業，因此引起各國的高度關注。

本次 GDPR 規範重點包括擴大適用範圍、加重企業責任、強化當事人權利及提高罰則金額等部分；另於個人資料國際傳輸係採取「原則禁止、例外允許」模式，

因此只有在符合 GDPR 規範的例外情形下，個人資料才能進行國際傳輸。鑑於臺歐雙邊經貿往來向來密切，GDPR 的施行勢必將廣泛影響我國在歐盟營運或對歐從事業務的企業，政府對此當積極推動相關措施，以協助企業因應 GDPR 的衝擊與影響。本文以下將簡介 GDPR 重點規範，並就政府因應措施及推動方向進行相關說明。

貳、歐盟 GDPR 簡介

歐盟 1995 年發布「個人資料保護指令」(Data Protection Directive) 係對於個人資料保護的最低限度規範，歐盟各會員國尚須以該指令為基礎並進一步內國法化，以建立各會員國的個人資料保護法制，惟各國內國法化後可能產

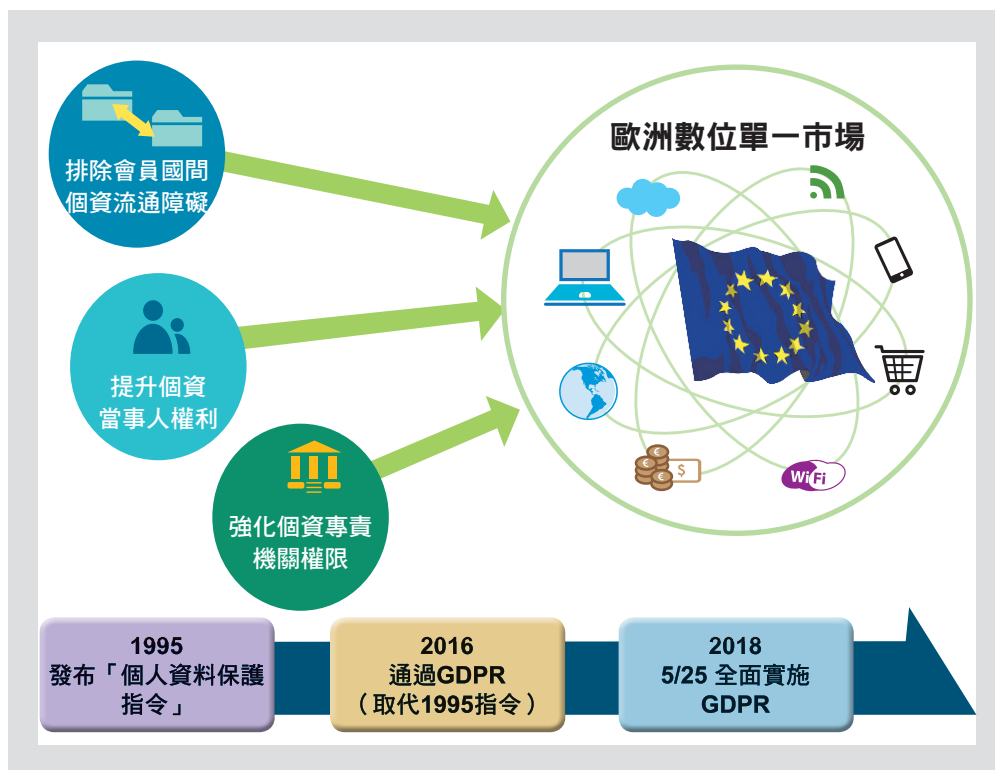


圖 1 一般資料保護規則 (GDPR) 背景說明

生規範上的落差，進而形成不利資料流通、阻礙經濟活動或造成不當競爭等負面影響。因此，歐盟於推動與建構數位單一市場之際，於 2016 年通過一般資料保護規則（General Data Protection Regulation, GDPR），在規範位階上將原有的「指令」（Directive）提升為「規則」（Regulation），這意味著各會員國縱使不透過內國法化的程序，仍可一體適用 GDPR 的規範，易言之，不論歐盟會員國是否將 GDPR 規定轉換成內國法，個資當事人都可以直接援引 GDPR 規定作為個資保護的主張。GDPR 經過 2 年過渡期後，已於今（2018）年 5 月 25 日全面施行，歐盟欲透過 GDPR 的實施，以達成排除會員國間個人資料流通障礙、提升個資當事人權利並強化個資專責機關權限等願景。

GDPR 重點規範說明如下：

一、擴大適用範圍

在適用範圍上，無論個資控管者（data controller）或受託處理者¹（data processor），只要符合下列三種情形之一且處理個人資料，就須受 GDPR 的規範：

（一）在歐盟境內²設立據點，且無論處理個資的行為是否發生在歐盟境內；或

¹ 我國個人資料保護法將個資的使用區分為蒐集、處理及利用等行為態樣，而 GDPR 則統稱為「processing」，本文於此統一使用「處理」的用語，其定義可觀諸 GDPR 第 4 條第 2 項規定「不論是否透過自動化方式，對個人資料或個人資料檔案執行任何操作或系列操作，例如蒐集、記錄、組織、結構化、儲存、改編或變更、檢索、查閱、使用、傳輸揭露、傳播或以其他方式使之得以調整或組合、限制、刪除或銷毀」。

² GDPR 適用範圍為歐洲經濟區（European Economic Area），因此除歐盟成員國外，尚包含冰島、列支敦斯登及挪威。

- (二) 在歐盟境內未設立據點，但對歐盟境內當事人提供商品或服務；或
- (三) 在歐盟境內未設立據點，但監控歐盟境內當事人於歐盟內的行為。

二、擴大個人資料定義

個人資料可區分為「一般個人資料」與「特種個人資料」。一般個人資料是指「有關識別或可得識別個資當事人的任何資訊」，而所謂「可得識別個資當事人」是指得以直接或間接地識別該個資當事人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該當事人的身體、生理、基因、心理、經濟、文化或社會地位等具體因素等。另在 GDPR 立法前言 (Recital) 更說明包含透過網路 IP 位址、瀏覽紀錄產生的數位軌跡並得追蹤識別特定當事人身分等皆屬之；特種個人資料是指「揭露人種、血統、政治意見、宗教、哲學信仰、工會身分、基因、生物特徵、健康相關、性生活與性傾向等資料」，且原則上禁止處理。

三、明確當事人同意

倘透過個資當事人同意而取得個人資料者，該「同意」必須是由個資當事人自由提供、具體、知情及明確同意，而單純沉默、預設選項為同意或當事人不為表示的情形，皆不該當為同意；且若個人資料的處理具有多重目的，應就全部目的取得同意。另應注意在個資當事人撤回同意方面，須提供如同給予同意一樣容易的方式使其撤回同意。

四、加重企業責任

(一) 書面委託歐盟境內代表

非設立於歐盟境內，但對於歐盟境內當事人提供商品或服務或監控其行

為者，除偶然性的處理或公務機關外，均應以書面委託歐盟境內的代理人作為代表，受理主管機關或個資當事人提出的要求。

(二) 個人資料保護設計及預設

應考量現有技術、執行成本及處理個人資料行為的性質、範圍、內容、目的及對當事人權益所生的不同風險等，在技術上及組織上納入隱私保護措施，以確保個人資料處理符合 GDPR 要求並保護個資當事人的權利。

(三) 個人資料侵害事故通報與通知

發生個人資料侵害事故，應於知悉後 72 小時內通報當地個人資料主管機關；若對個資當事人的權益有重大危害之虞，亦應通知該當事人。

(四) 個人資料保護影響評估

個人資料處理可能造成個資當事人高度風險者，應於處理前執行個人資料保護影響評估，尤其是大規模的個人特質評估、處理特殊類型或犯罪個人資料、監控公共領域者。

(五) 指定個人資料保護長

公務機關處理個人資料、或處理個人資料之核心業務涉及大規模監控個資當事人、或大規模處理特種個人資料與犯罪個人資料的情形，應指定個人資料保護長。因此企業是否應設置個人資料保護長，並非依據企業的規模大小，而是應視企業本身所涉及的業務而定。

(六) 紀錄個資處理責任

員工人數在 250 人以上的企業或組織，應負責維護資料處理活動之紀錄，惟員工人數低於 250 人的企業或組織，如係經常性處理個人資料或涉及處理特種或犯罪個人資料者，仍有該責任的適用。

五、強化當事人權利

(一) 拒絕權

倘處理個人資料的依據為「基於公共利益」或「基於正當利益」時，個資當事人有權依具體情形，隨時拒絕該等個人資料之處理，包含對個資當事人進行剖析（profiling）的行為。另倘係為直接行銷之目的而處理個人資料時，該個資當事人有權隨時拒絕為行銷而處理其個人資料，包括拒絕與該直接行銷有關範圍內的剖析行為。

(二) 更正權

個資當事人有權請求資料控管者即時更正不正確的個人資料，且慮及個人資料處理之目的，個資當事人有權請求補充其有欠缺的個人資料。

(三) 刪除權（被遺忘權）

在符合特定情形³下，個資當事人有權請求，且資料控管者亦有義務即時刪除個人資料或連結。

(四) 個人資料可攜權

在符合特定情形⁴下，個資當事人有權要求以「結構的」、「普遍使用的」、「機器可讀的」形式，接收其原提供予個資控管者的個人資料，並有權傳輸予其他控管者。

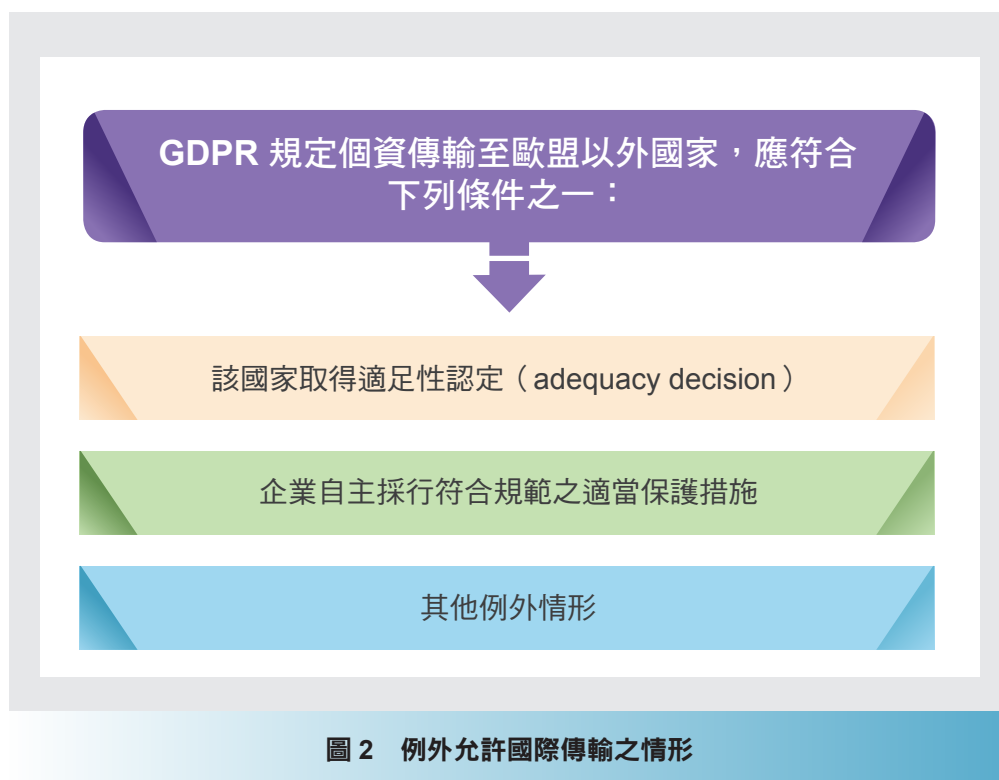
³ 包括 (1) 對於原本蒐集或處理個人資料之目的已無必要、(2) 個資當事人撤回同意，且無其他法律依據、(3) 個資當事人依 GDPR 規定對處理個人資料行為表示反對、(4) 個人資料遭違法處理、(5) 個資控管者依法律規定有義務刪除個人資料、(6) 個資控管者對兒少提供資訊社會服務等情形。

⁴ 包括 (1) 個資控管者處理個人資料的法律依據為「當事人同意」或「與當事人有契約關係」、(2) 個資控管者以自動化方式處理個人資料等情形。

六、個人資料國際傳輸

採取「原則禁止、例外允許」的模式，亦即只有符合例外規定的情形，始得進行個人資料的國際傳輸。而例外情形包括：

- (一) 國家或地區取得適足性認定 (adequacy decision)；或
- (二) 企業自主採行符合規範的適當保護措施，例如：標準個人資料保護契約條款 (Standard Contractual Clauses, SCC)、拘束性企業規則 (Binding Corporate Rules, BCR)、行為守則 (Codes of Conduct, CoC)、取得特定認證 (Certification) 等方式；或
- (三) 符合其他例外情形，例如：
 1. 告知個資當事人可能的風險後，取得當事人明確同意；



2. 因執行契約所必要；
 3. 基於公共利益的重要原因；
 4. 個資當事人無法為同意的表示，但移轉該個人資料對保護其重要利益實屬必要等情形；
- 惟應注意的是，上述其他例外允許國際傳輸的情形，適用前提為少量、偶發性的國際傳輸事件。

七、提高罰則金額

依不同的違法行為區分，最高可處以 1,000 萬歐元或（如為企業）全球營業總額 2% 的行政罰鍰；或最高 2,000 萬歐元或（如為企業）全球營業總額 4% 之行政罰鍰。

叁、我國政府因應推動方向

歐盟為我國第一大外資來源與第五大貿易夥伴，臺歐雙邊經貿往來向來密切，GDPR 的施行勢必將廣泛影響我國在歐盟營運或對歐從事業務的企業，面對 GDPR 的施行，我國當不能置身事外；而歐盟的個人資料保護法規向為各國個人資料保護法之立法典範，我國《個人資料保護法》（以下簡稱《個資法》）歷次修法亦多有參照其規範，對此，政府除持續關注 GDPR 的規定及後續施行概況外，於 GDPR 因應措施及推動方向，更應積極整合各部會辦理相關事宜。

國家發展委員會（下稱國發會）已透過成立個人資料保護專案辦公室、辦理與歐盟洽談適足性認定事宜、官網設置 GDPR 專區，並舉辦 GDPR 研討

會及多場宣導說明會等措施，以協助公、私部門因應 GDPR 可能帶來的衝擊與影響。分述如下：

一、成立「個人資料保護專案辦公室」

由於我國個人資料保護體系在監督機制上未設單一主管機關，而係採分散式管理，由非公務機關所屬之中央目的事業主管機關或直轄市、縣（市）政府為監督機關，因此面對 GDPR 全面施行，我國亟需一單位作為部會間協調整合的平臺，以統籌辦理相關因應事宜。國發會奉行政院指示，於今（107）年 7 月 4 日正式成立「個人資料保護專案辦公室」（以下簡稱個資辦公室），並自今年 7 月 25 日起，我國《個資法》的法律主政機關由法務部移交國發會職掌，一方面積極整合各部會辦理因應 GDPR 相關事宜，並向歐盟申請適足性認定，另方面協調整合並加強各部會落實執行《個資法》的一致性。未來個資辦公室亦將視歐盟國際傳輸適足性認定諮商進程，持續研議個人資料保護相關因應對策。

二、辦理與歐盟洽談適足性認定事宜

為協助我國企業與歐盟間得以自由進行個人資料國際傳輸，國發會陳主委已於今年 5 月底率團拜訪歐盟，正式表達我方申請適足性認定的意願，國發會隨即展開適足性認定的準備工作。目前個資辦公室刻依歐盟建議，參照 GDPR 規定、歐盟適足性認定參考文件⁵與歐盟法院判決⁶等資料，撰擬我國個人資料保護整體架構之自我評估報告，並召開多次專家諮詢會議討論適足性評估工作，以期後續與歐盟順利展開技術性對話，進而取得歐盟認可我國對個人資料保護具適足程度。

⁵ Article 29 Working Party, Adequacy Referential, WP 254 rev.01

⁶ 歐盟法院 SCHREMS 案判決。

三、官網設置GDPR專區

國發會已於官網設置 GDPR 專區（圖 3），提供 GDPR 簡介、導讀、法規翻譯、歐洲資料保護委員會（EDPB）採認之 GDPR 相關解釋文件、GDPR 與我國《個資法》重點比較分析以及相關部會諮詢窗口等，並將適時更新文件，以提供各界參考運用。

首頁 > 主要業務 > 法制協調 > 個人資料保護專案辦公室 > 歐盟一般資料保護規則專區

歐盟一般資料保護規則專區

隨著數位經濟科技發展與全球化影響，個人資料保護議題帶來許多新的挑戰，歐盟為提升個人資料保護規範密度，並建立歐盟境內一體適用之管理規範，於2016年5月24日通過「一般資料保護規則」(General Data Protection Regulation, GDPR)，以取代歐盟1995年個人資料保護指令(Data Protection Directive)，並自今(2018)年5月25日全面施行。

為因應GDPR施行後可能造成之衝擊與影響，本會已於今年4月間邀集各部會積極研議相關因應策略，為利各界瞭解GDPR相關重要資訊，爰建置本網頁，並提供GDPR簡介、翻譯資料、相關部會諮詢窗口以及GDPR與我國個人資料保護法之比較分析，相關資訊將隨時更新。

- ▶ 歐盟GDPR簡介
- ▶ 歐盟GDPR導讀
- ▶ 歐盟GDPR法規
- ▶ 歐盟GDPR與我國個人資料保護法之重點比較分析


圖 3 國發會官網設置 GDPR 專區

四、舉辦GDPR研討會及多場宣導說明會

為提升公、私部門對於 GDPR 的瞭解，國發會於今年 8 月舉辦中央及地方機關之 GDPR 研討會，並於 9 月舉辦北、中、南區 GDPR 企業宣導說明會，邀請相關部會分享 GDPR 因應作為以及專家學者進行專題演講，分別就政府面與產業面說明 GDPR 因應及調適方向，並透過綜合座談釐清各界對 GDPR 的相關疑義。

肆、結語

隨著數位經濟的科技發展以及全球化的影響，人類的生活步調逐漸發生變化，尤其是網際網路的普及、快速的資訊傳輸與大數據運用，為生活帶來許多便利，同時也產生相應的風險與挑戰，其中隱私權與個人資料的保護，儼然成為國際上面臨的重要議題。而當企業面對號稱史上最嚴格的 GDPR，或許擔心違反 GDPR 可能被處高額罰鍰、亦或害怕未遵守 GDPR 可能對其商譽造成影響，政府宜積極協助與輔導企業瞭解與掌握 GDPR，以有所因應，除整體落實個人資料的保護外，並避免造成不必要的恐慌。

有鑑於此，在政府協助企業因應 GDPR 方面，除有賴各中央目的事業主管機關就其所轄產業提供相關輔導與諮詢外，同時為補足我國目前個資保護採取的分散式管理機制所缺乏的協調與整合功能，政府亦已成立「個人資料保護專案辦公室」，以統籌各部會辦理 GDPR 因應相關事宜，並將持續與歐盟洽談國際傳輸適足性認定，未來亦配合推展進程適時檢討我國《個資法》。



專題報導

REPORT

政府與產業因應GDPR之調適措施

資訊工業策進會科技法律研究所 戴豪君、林其樺*

- 壹、前言
- 貳、GDPR 資料跨境傳輸相關規範
- 參、國家層次溝通適足性認定暨產業自我規律措施
- 肆、個人資料外洩之通知
- 伍、結論

壹、前言

歐盟個人資料保護立法自 1995 年公布之資料保護指令 (Data Protection Directive)，旨在確保人民隱私基本權。由於指令所要求事項，對會員國具有拘束力。惟其執行之形式與方法，得由會員國自行決定，各會員國有不同執行方式，導致對於歐盟法律之遵循更顯複雜、不確定。且就立法時間背景來看，許多新興網路服務型態諸如社群網站 (social networking sites)、雲端運算 (cloud computing)、行動定位服務 (location-based services,

* 戴豪君博士為資策會科技法律研究所資深研究員，林其樺為該所專案經理。

LBS) 均不若今日普及與活絡，所衍生個人資料保護議題並未為立法所涵蓋。為了確保個人資料保護之基本權利（歐盟基本權利憲章第 8 條）獲得實現，同時考量將來數位經濟的發展，歐盟對個人資料規範進行重新檢視，由歐洲議會（European Parliament）及歐盟理事會（European Council）於 2015 年完成修正個人資料保護相關規範，一般資料保護規則（General Data Protection Regulation, Regulation, GDPR）¹。因應 GDPR 的施行，歐盟設立歐洲資料保護委員會（European Data Protection Board, EDPB）²。EDPB 首任主席 Andrea Jelinek，在 2018 年 5 月 25 日第一次會議中表示：在個人資料常被視為貨幣的世界中，個人權利經常被忽視或蔑視。我們不能忘記個人資料係來自人類的事實，GDPR 將賦予個人資料與主管機關有效保護與落實基本人權³。

歐盟 GDPR⁴ 規範重點主要為：重申當事人權利、深化歐盟內部市場、確保規範更確實落實、具合法性基礎之國際傳輸，以及建立全世界統一性之資料保護標準。使當事人之個人資料於傳輸、處理或保存上，即便在歐盟境外或虛

¹ EU Press Release Database, Building on modern and unified rules to strengthen fundamental rights and create a Digital Single Market - Joint Statement by Vice-President Ansip and Commissioner Jourová on the occasion of the 2016 Data Protection day, http://europa.eu/rapid/press-release_STATEMENT-16-181_en.htm, (last visited Sep. 24, 2018).

² 依 GDPR 第 70 條第 1 項規定 EDPB 為 GDPR 之獨立專責機關。EDPB 由歐洲資料保護監督機關 (European Data Protection Supervisor, EDPS)、各會員國之資料保護主管機關 (Data Protection Authority, DPA)，以及歐盟執委會 (European Commission) 所組成，惟其中執委會不具投票權。See EDPB, Memorandum of Understanding between the European Data Protection Board and the European Data Protection Supervisor, https://edpb.europa.eu/sites/edpb/files/files/file1/memorandum_of_understanding_signed_en.pdf (last visited July 15, 2018).

³ Europe's new data protection rules and the EDPB: giving individuals greater control, https://edpb.europa.eu/news/news/2018/europes-new-data-protection-rules-and-edpb-giving-individuals-greater-control_pt (last visited Sep. 23, 2018)

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

擬網路上，均受到保護。對資料當事人而言，對於自身個人資料將有更多自主控制權，且有更易查詢、取得之管道⁵。

本文將介紹歐盟 GDPR 對歐洲經濟區（European Economic Area, EEA）境外國家與產業資料跨境傳輸之相關規範，觀察個人資料跨境傳輸應注意的問題，最後總結境外國家與產業調適措施以及事故疑慮應變措施，提供我國因應 GDPR 之參考。

貳、GDPR 資料跨境傳輸相關規範

GDPR 資料跨境傳輸規定在第五章關於個人資料傳輸至第三國或國際組織之相關規定（CHAPTER V Transfers of Personal Data to Third Countries or International Organisations）第 44 條至第 50 條。歐盟 GDPR 資料跨境傳輸規範如表 1。

國際上關於資料跨境傳輸之限制規範，大多未以資料在地化之文字直接明訂於法規中，但於法律中明文跨境傳輸之規範，並表明該國對於資料跨境傳輸之態度。同時未全面禁止資料跨境自由流通，法律規範於特定條件下仍得進行資料跨境傳輸，例如歐盟跨境傳輸規定資料接收國，應提供個人資料適當保護水準，或提供適當的安全維護措施，且給予資料當事人權利可執行並有效救濟途徑。

⁵ 據歐盟 2016 年之調查，十分之九歐洲人都曾對行動 apps 未經同意蒐集其個人資料的狀況表示擔心；另外，十分之七歐洲人認為公司於個人資料利用可能有洩漏疑慮。關於這些爭議，GDPR 修正便係以強化公民基本權利並建立信心，並提供工具使當事人更能控制其個人資料。

See, EU Press Release Database, Questions and Answers – Data protection reform, http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm (last visited Sept. 22, 2018).

表 1 歐盟 GDPR 資料跨境傳輸規範

歐盟資料跨境傳輸規範	一般資料保護規則 (General Data Protection Regulation, GDPR)
規範章節	第五章 個人資料傳輸至第三國或國際組織之相關規定 (CHAPTER V Transfers of Personal Data to Third Countries or International Organisations) (第44條至第50條)
原則：限制	個人資料傳輸至第三國或國際組織，僅於執委會 (European Commission) 決定該第三國或國際組織確實達到「適當的保護水準」(an adequate level of protection) 時，方得為之 (第45條第1項)。
例外	<ol style="list-style-type: none"> 1. 國家層次之適足性認定 (adequacy decision)，由歐盟執委會認定第三國已達到適當保護 (第45條)。 2. 資料控制者、處理者自我規律，提供適當安全維護措施 (第46條第2、3項)。 <ol style="list-style-type: none"> (1) 與公務機關間或機構間有法律拘束力且得執行之協議 (instrument)。 (2) 具拘束力企業規則 (Binding Corporate Rules, BCRs) (第47條)。 (3) 標準契約條款 (Standard Contractual Clauses, SCC) (第28條)。 (4) 行為準則 (code of conduct) (第40條)。 (5) 認證機制 (certification mechanism) (第42條)。 3. 特別規定 (derogation)，如取得當事人同意或契約約定 (第49條第1項)。 4. 為重大公共利益、法院行使司法權等規範 (第49條第1項)。
適用範圍	域外效力：非設立於歐盟境內之資料控制者或處理者，對於歐盟境內之資料主體提供商品或服務，或於歐盟內所為行為之監控 (第3條第2項)，有GDPR之適用。

資料來源：本文自行整理。

為促進資料得以跨境傳輸，需透過建立資料自由流通之環境達成，如歐盟為發展資料經濟 (data economy) 政策，為能發揮資料應用之潛力，必須解決阻礙資料自由流通 (the free flow of data) 的障礙⁶，確保資料跨境傳輸與應用。如今歐盟 GDPR 已正式上路，在資料保護指令時期，職司發布指導

⁶ Building a European data economy, EUROPEAN COMMISSION, <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy> (last visited Jan. 13, 2018) .

方針 (Guidelines)，提供隱私與資料保護諮詢之第 29 條工作小組 (Article 29 Working Party, WP29)，由歐洲資料保護委員會 (EDPB) 取代。EDPB 將透過指導方針、諮詢意見 (Opinion)⁷ 和具拘束力裁定⁸ 等途徑，確保歐盟資料保護相關規範之落實，並促使歐盟會員國資料保護主管機關 (Data Protection Authority, DPA) 間有效合作。

延續指令時期 WP29 之工作，EDPB 會持續針對 GDPR 規範議題，提供指導方針供資料保護主管機關 (DPA) 落實參考。原由 WP29 作成之指導方針已為 EDPB 所採納，仍為有效文件⁹，茲整理歐盟 GDPR 有關指導文件如表 2。

叁、國家層次溝通適足性認定暨產業自我規律措施

歐盟資料傳輸至第三國仍採原則禁止，僅於符合特定情形時，得例外進行資料跨境傳輸。特定情形即包含國家層次之適足性認定或國際協定。GDPR 適足性認定係由執委會認定第三國資料保護程度是否符合適當的保護水準，須確保第三國提供的保護水準是「本質相當於歐盟之保護」(essentially equivalent to that ensured within the Union)，且第三國應提供資料有效與可執行的權利與方式。GDPR 第 45 條第 2 項規定執委會於評估適當保護時，應考量下列因素：

⁷ 例如依 GDPR 第 40 條第 7 項規定，如企業所擬之行為準則 (Code of Conduct) 涉及數會員國之資料處理行為時，有關 DPA 得將行為準則草案送至 EDPB，EDPB 應就該草案是否合於 GDPR 提出諮詢意見。

⁸ 相較於 WP29，具拘束力裁定為 EDPB 新職掌範圍。需 EDPB 裁定之情境，例如資料跨境處理之爭端，歐盟有關 DPA 無法取得爭端解決之共識時，將由 EDPB 作成裁定，該裁定將對有關 DPA 產生拘束力。See European Commission, EU Data Protection Reform, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-role-edpb_en.pdf (last visited July 15, 2018).

⁹ EDPB, Endorsement of GDPR WP29 guidelines by the EDPB, <https://edpb.europa.eu/node/89> (last visited July 15, 2018).

表 2 歐盟一般資料保護規則 (GDPR) 指導文件一覽表

序號	指導文件 (Guidelines)	備註
1	資料可攜權 (the right to Data Portability)	<ul style="list-style-type: none"> last Revised and adopted on 5 April 2017 WP242rev.01
2	資料保護長 (Data Protection Officers, DPOs)	<ul style="list-style-type: none"> last Revised and Adopted on 5 April 2017 WP243rev.01
3	認定資料控制者或資料處理者主責主管機關 (identifying a controller or processor's lead supervisory authority)	<ul style="list-style-type: none"> last Revised and Adopted on 5 April 2017 WP244rev.01
4	資料保護影響評估 (Data Protection Impact Assessment, DPIA)	<ul style="list-style-type: none"> last Revised and Adopted on 4 October 2017 WP 248 rev.01
5	個人資料違反通知 (Personal data breach notification)	<ul style="list-style-type: none"> last Revised and Adopted on 6 February 2018 WP250rev.01
6	自動化個人決策與分析 (Automated individual decision-making and Profiling)	<ul style="list-style-type: none"> last Revised and Adopted on 6 February 2018 WP251rev.01
7	行政罰款之設定及適用 (the application and setting of administrative fines)	<ul style="list-style-type: none"> Adopted on 3 October 2017 WP 253
8	同意 (Consent under Regulation)	<ul style="list-style-type: none"> last Revised and Adopted on 10 April 2018 WP259rev.01
9	透明性 (Transparency)	<ul style="list-style-type: none"> last Revised and Adopted on 11 April 2018 WP260rev.01
10	驗證及驗證要件 (Certification and identifying certification criteria)	<ul style="list-style-type: none"> Adopted on 25 May 2018 Guidelines 1/2018
11	第49條特別規定 (derogations of Article 49)	<ul style="list-style-type: none"> Adopted on 25 May 2018 Guidelines 2/2018

註：序號按文件編號排序。指導文件更新至 2018 年 7 月。

資料來源：歐洲資料保護委員會 (EDPB) 官網 (2018)。

- (一) 對人權與基本自由之尊重、相關法規，包括國家安全及刑法、公務機關對個人資料之近用權及該等立法、資料保護相關規則及安全維護措施之執行，第三國或國際組織之規則、判例法及資料主體行政與司法救濟；
- (二) 第三國內有獨立主管機關並有效運作，或對象為國際組織時，確保及執行資料保護規則之遵守，並與會員國主管機關合作；
- (三) 第三國或國際組織所加入之國際協定，或其他因具法律拘束力之契約或辦法、及從其參與多邊或區域體系而生之義務。

截至 2018 年，歐盟境外共有 12 個國家通過適足性認定 (adequacy decision)，包括安道爾共和國 (Andorra)、阿根廷 (Argentina)、加拿大商業性企業 (Canada) (commercial organisations)、法羅群島 (Faroe Islands)、根西 (Guernsey)、愛爾蘭 (Israel)、馬恩島 (Isle of Man)、澤西 (Jersey)、紐西蘭 (New Zealand)、瑞士 (Switzerland)、烏拉圭 (Uruguay)。另美國與歐盟簽訂有隱私盾協議 (Privacy Shield framework)¹⁰。

在欠缺提供適當保護之決定時，資料控制者或處理者應採取適當安全維護措施，以彌補第三國對資料保護之欠缺。我國仍在爭取 GDPR 適足性認定之過程中，與歐盟之資料跨境傳輸，建議產業依組織型態、營運模式規劃自我規律措施。以標準契約條款 (SCC) 以及具拘束力契約規則 (BCRs) 為例：

¹⁰ Commission decisions on the adequacy of the protection of personal data in third countries, European COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (last visited Jan. 2, 2018) .

(一) 標準契約條款

個人資料之國際傳輸，如無法取得資料當事人 (data subject) 同意，原則上應禁止該個人資料之國際傳輸，然企業如簽訂合約訂定標準契約條款 (SCC)，得例外為之。例如由我國業者提供整體運輸工具租賃系統，由歐盟境內運輸工具租賃業者提供消費者服務，並將系統資料交由我國業者處理。此時歐盟業者與我國業者可簽訂規範歐盟控管者傳送資料到非歐盟或歐洲經濟區處理者之 SCC。

是否訂定 SCC，通常取決於企業的意願，主要考量因素有：

1. 反映最終承擔風險。即標準契約條款下，損害發生時，由於違反第三方受益人條款 (third party beneficiary clause)，傳輸方以及被傳輸方須負連帶責任；
2. 國際傳輸行為本身具合法性基礎，例如依據法定職權等；
3. SCC 可適用在歐盟與其他國家間之國際傳輸；
4. 企業須各自與歐盟傳輸方簽締合約；
5. 標準契約條款協商通常需要花費一定時間、成本。

(二) 具拘束力企業規則

具拘束力企業規則 (Binding Corporate Rules, BCRs) 內容類似於行為準則，由多國企業組成之團體共同協商而訂。BCRs 效力範圍可及於從事共同經濟活動 (a joint economic activity) 集團內所有企業，一般由該企業集團向歐洲總部的所在地，或負責處理個人資料保護部門所在地。或負責執行 BCRs 的部門所在地等個人資料主管機關申請，並由主責主管機關 (LSA) 遵循一致性原則決定程序進行審核批准。

簽訂 BCRs 的好處，在於以下數點：

1. 遵守 GDPR 第 47 條規定；
2. 團體內個人資料保護的實務操作得以進行統一協調；
3. 避免國際傳輸產生之風險；
4. 無須每次傳輸便簽署合約；
5. 可以在企業內部資料保護政策外進行溝通，有利協調國際傳輸產生的制度落差；
6. 企業個人資料管理有具體參照方向；
7. 讓資料保護落實於企業持續營運；
8. 取得 BCRs 通常有助於提升企業保障個人資料形象。

此外，EDPB 最新之「第 49 條特別規定指導文件」¹¹ 亦與第三國資料跨境傳輸有關。歐盟境外企業，如所在地國家尚未通過適足性認定（adequacy decision），或企業本身資料保護適當安全措施尚未完全合於 GDPR 第 46 條要求，且未申請「具拘束力企業規則」（BCRs）時。GDPR 第 49 條第 1 項規定於特定情形下（包括已得資料當事人明確同意、為重大公共利益等 7 種情形），仍得進行第三國資料跨境傳輸。但要留意的是，企業得否援引 GDPR 第 49 條，EDPB 提出二階段判準（two-step test）：

- （一）不違背 GDPR 第 5、6 條揭示之原則；
- （二）傳輸行為合於第 5 章第三國資料跨境傳輸規範宗旨。¹² 資料跨境傳輸行為須屬「偶發且非常態性」（occasional and not repetitive transfers）且符合「必要性」（necessary）時，始得主張適用。

¹¹ Guidelines 2/2018 on derogations of Article 49 under Regulation (Guidelines 2/2018).

¹² Id., at 3-4.

以當事人明確同意為例，如有歐盟企業基於產品提供目的蒐集消費者個人資料，嗣後偶然有跨境提供個人資料需求時，該歐盟企業須另行告知消費者有第三國資料跨境傳輸情事，明確說明該第三國非適足性認定國家、資料處理原則，以及資料當事人權利可能無法於第三國主張等資訊，使消費者得以自行判斷資料跨境傳輸風險，進而提供明確、特定的知情同意¹³。

肆、個人資料外洩之通知

資料處理、利用過程中，往往伴隨著隱私風險，個人資料外洩也不易為資料當事人所察覺。為讓資料當事人得於第一時間了解其可能受影響權利，以及如何應對，GDPR 第 34 條第 1 項規定：「當個人資料外洩可能對自然人的權利和自由造成高度風險時，資料控制者應即時將個人資料外洩通知資料當事人」¹⁴，以「可能造成高風險」為通知資料當事人的判斷門檻。個人資料外洩，係指「資料控制者違反個人資料傳輸、儲存等安全處理要求，意外或不法致個人資料遭毀損、遺失、變更，或遭未授權揭露、近用」¹⁵。對於資料控制者如何判斷資料外洩風險以實踐外洩通知，歐盟於 2017 年提出了個人資料外洩通知指引（Guidelines on Personal Data Breach Notification under Regulation 2016/679）¹⁶，就 GDPR 個人資料外洩通知指引（以下簡稱個資外洩指引）規定重要概念加以闡述與釐清。

¹³ Id., at 6-8.

¹⁴ “When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, THE controller shall communicate the personal data breach to the data subject without undue delay.” Commission Regulation 2016/679, art. 34(1), 2016 O.J. (L 119) 1, 52.

¹⁵ “A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or ACCESS to, personal data transmitted, stored or otherwise processed.” Commission Regulation 2016/679, art. 4(12), 2016 O.J. (L 119) 1, 34.

¹⁶ Article 29 DATA Protection Working Party [Art. 29 WP], Guidelines on Personal Data Breach Notification under Regulation 2016/579, 17/EN, WP250 (Oct. 3, 2017), available at file:///D:/User/Downloads/20171013_wp250_enpdf.pdf (last visited Sept. 27, 2018).

個人資料外洩的風險類型大致分為三類：

- (一) 機密性違反疑慮 (confidentiality breach)：主要係指個人資料意外地或未經授權遭取得或揭露之情況；
- (二) 可及性違反疑慮 (availability breach)：指個人資料意外地或未經授權遭毀損或滅失，致資料無法被近用之情況；
- (三) 完整性違反疑慮 (integrity breach)：則係指個人資料意外地或未經授權遭變更之情況¹⁷。

個人資料外洩通知對象，GDPR 區分資料監督主管機關 (supervisory authority) 以及資料當事人，分別規定於 GDPR 第 33 條與第 34 條。二者主要依資料外洩風險實現可能性區分通知對象：如資料控制者有合理程度 (a reasonable degree of certainty)¹⁸ 認定個人資料外洩會對自然人權利、自由構成隱私風險時，須於 72 小時內通報資料監督主管機關；如若認定隱私風險顯有可能實現 (high risk)，除非符合例外情況，否則應即時通知資料當事人。個資外洩指引指出資料控制者要依 GDPR 第 46 條規定通報主責主管機關 (Lead Supervisory Authority, LSA)，該 LSA 之擇定應載明於資安事故緊急應變計畫；或由企業依 GDPR 第 27 條於歐盟境內指定的代表，向其所在會員國之主管機關進行通報。

考量資料處理者於個人資料處理亦舉足輕重，應進行個人資料外洩通知者，除前述資料控制者外，資料處理者亦肩負協助資料控制者履行 GDPR 資料安全處理之義務¹⁹。因通知法律責任仍歸屬於資料控制者，建議企業如有資料委託處理需求時，妥善與受委託方約定相關因應措施。

¹⁷ Id., at 6.

¹⁸ Id., at 9.

¹⁹ 依據 GDPR 第 28(3)(f) 條規定，資料控制者與資料處理者間之契約，應包含 GDPR 第 32 條至第 36 條。由次可知，資料處理者有協助資料控制者履行個人資料外洩通知之義務。

個人資料外洩疑慮通知內容，至少應包含：

- (一) 個人資料外洩情事，說明受影響群體（如消費者、受雇者等）、人數，及個人資料種類與數量；
- (二) 資料保護長等聯繫窗口；
- (三) 個人資料外洩可能影響；
- (四) 資料控制者所採取因應措施。²⁰

必要時資料監督機關得要求資料控制者提供進一步資訊²¹。

伍、結論

我國《個人資料保護法》（以下簡稱《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。」資料隱私保護與合理利用之權衡，向來為《個資法》重要命題。特別是資料經濟價值彰顯後，資料之利用，甚至跨境傳輸等目的外利用，為實務上所常見。

我國個人資料國際傳輸之規範，就非公務機關個人資料國際傳輸採取原則開放，例外限制。依《個資法》第 21 條規定，企業之個人資料國際傳輸有下

²⁰ “The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.” Commission Regulation 2016/679, art. 33(3), 2016 O.J. (L 119) 1, 52.

²¹ Supra note 16, at 12.

列 4 種情形之一者，中央目的事業主管機關得限制之：涉及國家重大利益、國際條約或協定有特別規定、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、以迂迴方法向第三國（地區）傳輸個人資料規避本法。我國目前在資料國際傳輸相關函釋僅 2 則：


（一）國家通訊傳播委員會通（NCC）2012 年 9 月通傳通訊字第 10141050780 號：限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區，衡酌大陸地區之個人資料保護法令尚未完備，通訊傳播事業於國際傳遞及利用個人資料時，應考量接受國家或地區對個人資料有完善之保護法令，爰依「電腦處理個人資料保護法」第 24 條第 3 款規定，限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區。

（二）法務部 102 年 6 月 6 日法律字第 10100088140 號函要義：按「國際傳輸」係指將個人資料作跨國（境）之處理或利用（《個資法》第 2 條第 9 款規定）。故除中央目的事業主管機關依《個資法》第 21 條規定限制非公務機關為國際傳輸個人資料之行為外，非公務機關若屬機關內部之資料傳送（屬資料處理），例如：基於同一法人人格性質，總公司將資料傳送給分公司、公務機關將資料傳送給國外辦事處等，於符合《個資法》第 19 條（例如：法律明文規定、與當事人有契約關係等）或第 20 條第 1 項本文規定，即得於特定目的必要範圍內將個人資料作為跨國（境）之處理或利用，與國際傳輸過程是否符合保密原則無涉。另若將資料國

際傳輸提供當事人以外第三人（屬資料利用），例如：母公司將資料提供給子公司或他公司，則應注意是否符合《個資法》第 20 條第 1 項但書有關特定目的外利用之要件（例如：當事人書面同意）。

此外，《個資法》未設單一主管機關而採分散管理制度，資料跨境傳輸之實務處理，由各目的事業主管機關審酌。行政院於 2018 年 7 月指示國發會正式成立「個人資料保護專案辦公室」，以協調整合部會辦理 GDPR 相關因應事宜。值此過渡期間，我國較可能受 GDPR 實施影響產業（例如金融業、電子商務以及航空公司等），金管會、經濟部以及交通部等相關部會，都已著手輔導企業符合相關的規定；以公股行庫為例，金管會以透過專業顧問服務等來協助金融業者建置法遵規範，並設置資料保護長等，符合 GDPR 的規定。且臺灣於 2018 年 5 月 21 日通過亞洲太平洋經濟合作會議（APEC）的跨境隱私保護體系（CBPR）第一階段審查。儘管 APEC CBPR 體系不若歐盟 GDPR 嚴格，但 APEC 也正在力推與歐盟 GDPR 接軌互通，我國若能加入 CBPR 體系，將有助於我國業者進一步整備符合歐盟標準。

考量我國目前尚非歐盟承認之適足性認定名單，企業產品與服務提供除考量採取 SCC 或 BCRs 外，如認屬歐盟 GDPR 第 49 條規範情形時，建議參考 EDPB「第 49 條特別規定指導文件」，檢視決策是否合於 GDPR 資料保護原則，並評估既有個人資料保護管理程序暨措施。為強化企業資料治理以保障個人隱私，資料跨境傳輸行為如係基於法定要求，或涉及高風險，抑或處理方法顯著變更時，如何確保資料依其揭露方式無從識別，或者對於當事人權益「始終」有利，建議參考歐盟 2017 年 10 月配套提出之「資料保護影響評估」（Data protection impact assessments, DPIA）指導文件進行影響評估²²，在開始處理資料之前，確保個人資料處理對於資料當事人之影響及公平性，資料隱私風險識別、風險門檻控管之自我審查（self-censoring）方向。

最後，歐盟 GDPR 要求資料控制者如發現個人資料管理過程中有外洩風險時，應即著手調查，認定後盡快進行個人資料外洩通知，並採取相應措施，以有效控管隱私風險，維護資料當事人權益同時，亦能加深資料控制者與資料當事人間之信賴。對照我國《個資法》第 12 條個人資料外洩通知規定，主要仍在防免事故擴大，相較於歐盟 GDPR 從外洩疑慮開始掌握風險，事後的事務因應須更即時、確實反映，此為企業因應 GDPR 中須思考的問題。

²² Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679/17/EN(WP248 rev. 01).

GDPR之國際傳輸

國發會法制協調中心

壹、GDPR 之國際傳輸規定

貳、GDPR 適足性認定

參、小結

GDPR 對歐洲經濟區（European Economic Area）內個人資料（以下簡稱個資）提供相當完整之保護規範，但在國際化與網路化之時代，個資之國際傳輸為不可避免之情形，為使 GDPR 對個資之保護可延伸至個資所到之處，GDPR 規定歐盟個資傳輸至第三國或國際組織時，僅於該國或國際組織已遵循 GDPR 之前提下，始得為之。

本文將就 GDPR 國際傳輸之規定、以及國際傳輸規定中由國家取得適足性認定之規定與要求分別予以說明。

壹、GDPR之國際傳輸規定

GDPR 對於個資之國際傳輸規定於第五章「個資傳輸至第三國或國際組織」，採「原則禁止、例外允許」之立法模式，例外允許國際傳輸之情形包括三種情形，其一為由第三國或國際組織取得歐盟執委會之適足性認定，其二為由企業自主採行符合 GDPR 規定的適當保護措施，如標準個資保護契約條款、拘束性企業規則、行為守則、認證等，其三為其他特殊例外情形。

一、一般原則¹

依 GDPR 規定，對於歐洲經濟區個資之保護程度不應因國際傳輸而降低，是以歐洲經濟區個資之國際傳輸，不論是處理²中或擬於傳輸至第三國或國際組織再為處理者，僅於符合 GDPR 規定之情形下始得為之，包括個資從該第三國或國際組織再為之國際傳輸亦需適用，以確保 GDPR 對個資當事人之保護程度不受減損。

二、由第三國或國際組織取得適足性認定³

歐洲經濟區個資傳輸至第三國或國際組織，倘經歐盟執委會認定該第三國、該國之特定部門或該國際組織之個資保護已達充足程度且與歐盟之保護程度實質相當時，則歐洲經濟區個資可自由傳輸至取得適足性認定之該第三國、該國之特定部門或該國際組織。

執委會於評估適足性時，應考量該第三國、該國之特定部門或該國際組織之下列因素：

- 法規、對人權與基本自由之尊重，及有關公共安全、國防、國家安全、刑法、公務機關對個資接近使用權之個資保護規定及安全措施之執行，包括個資再向其他國家或國際組織為傳輸之法規、判例法、當事人權利及其行政與司法救濟途徑；
- 該國應有一個以上獨立監管機關並有效運作，如為國際組織時，應能確保及執行個資保護規定；應有協助及建議個資當事人行使其權利之執行權限，並與歐盟會員國之監管機關合作；

¹ 詳參 GDPR 第 44 條。

² GDPR 條文所稱之處理，相當於我國個資法之蒐集、處理、利用。GDPR 第 4 條第 2 項規定，「處理」(processing) 係指對個資或個資檔案為任何使用或一系列使用，不問是否透過自動化方式，例如蒐集、記錄、組織化、結構化、儲存、改編或變更、檢索、查閱、利用、傳輸揭露、傳播或以其他方式使之得以被取得、調整或組合、限制、刪除或銷毀。

³ 詳參 GDPR 第 45 條。

- 該國或國際組織所加入涉及個資保護之國際協定、具法律拘束力之公約或協議、參與多邊或區域體系而生之義務。

經歐盟執委會認定取得適足性之國家或國際組織，仍應受至少每 4 年一次之定期檢驗，確認其是否仍符合個資適足保護程度，執委會亦得撤銷、修改、暫停原取得之適足性認定，並公布名單。

三、企業自主採行適當保護措施

在未取得前述適足性認定之情形下，歐洲經濟區內之控管者或受託處理者欲將個資傳輸至第三國或國際組織時，應採取 GDPR 所定之適當保護措施始得為之，該保護措施應確保符合個資保護之要求、個資當事人可實現之權利以及有效之法律救濟，包括在歐盟或第三國均可獲得有效的行政或司法救濟並請求賠償。

企業自主採行之適當保護措施包括標準個資保護契約條款、拘束性企業規則、行為守則、認證等 4 種，以下分述之：

（一）標準個資保護契約條款

標準個資保護契約條款包括由執委會採行或由監管機關採行之版本⁴，目前執委會仍採行 1995 年個人資料保護指令時代所公布，包括由歐盟控管者傳予非歐盟地區之控管者，與由歐盟控管者傳輸予非歐盟地區之受託處理者等共 3 種版本⁵。

（二）拘束性企業規則

拘束性企業規則適用於跨國企業集團間或從事共同經濟活動之企業團體

⁴ 詳參 GDPR 立法前言第 108 點。

⁵ 詳參下列網址

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

間，就其個資保護政策，擬定內部遵守之規範，並須經監管機關核准。

拘束性企業規則須為具法律上拘束性並由共同經濟活動中之各事業團體成員適用與遵守，內容包括⁶：

- 集團及其各成員之組織與聯絡方式；
- 國際傳輸個資之類型、處理之類型及目的、受影響之個資當事人類型、及傳輸之第三國為何；
- 集團內部及外部具合法拘束力；
- 一般個資保護原則之適用，包括目的拘束原則、個資最少蒐集原則、個資品質、個資保護之設計與預設、個資處理之法律依據、特種個資之處理、確保個資安全之措施、及再傳輸至非受該拘束性企業規則所拘束之機構時之規定；
- 個資當事人關於處理之權利及行使該權利之方式，包括拒絕僅受自動化處理決定之權利、向監管機關及會員國之管轄法院提起申訴、及因拘束性企業規則之侵害而獲得賠償之權利；
- 設立於會員國之控管者或處理者承受其歐盟境外之成員任何違反拘束性企業規則時之責任，如能證明該境外成員對損害結果無須負責時，控管者或處理者得免除全部或部分責任；
- 個資保護長或團體內負責監督拘束性企業規則之遵守情形、監督培訓及處理申訴之人員或單位；集團確保拘束性企業規則遵循之驗證機制，包括個資保護審查及確保糾正措施以保護個資當事人權利之方

⁶ 詳參 GDPR 第 47 條。

法。驗證結果應通知上述專人或專責單位及集團之管理階層，並應於監管機關要求時提供；

- 申訴程序；
- 拘束性企業規則變更時應為紀錄並向監管機關報告；
- 與監管機關之合作機制，以確保集團成員之遵循；
- 於集團成員可能對拘束性企業規則有實質不利影響時，向監管機關報告；
- 針對長期或定期接觸個資之人員之適當個資保護訓練。

（三）行為守則⁷

GDPR 規定會員國、監管機關、委員會及執委會應鼓勵特定行業、中小微型企業採用行為守則，並應考量中小微型企業之需求。行為守則適用於國際傳輸時，控管者或受託處理者應透過契約或其他具有法律拘束力之文書，做成具有拘束力且可得執行之承諾，以適用該等適當保護措施。行為守則內容應包括：公正及透明之個資處理、控管者於具體情況下追求之正當利益、個資之蒐集、個資之假名化、提供大眾及個資當事人之資訊、個資當事人權利之行使、向兒童提供之資訊及對於兒童之保護，以及獲得其法定代理人同意之方式、個資保護之設計及預設之方式及程序，及確保處理安全性之保護措施、向監管機關及個資當事人通知個資之侵害、個資傳輸至第三國或國際組織、訴訟外紛爭解決機制。

⁷ 詳參 GDPR 第 40、41 條。

行為守則由協會或代表特定資料處理活動之機構訂定或修正，須先提交至主要監管機關，經監管機關確認該行為守則已提供適當保護措施者，監管機關即應核准，倘該行為守則無涉其他歐盟會員國者，監管機關並應為登記並公布，倘涉及多個會員國之處理活動者，監管機關應提交至個資保護委員會，評估是否符合 GDPR 並已提供適當保護，經個資保護委員會確認後，應將其意見提交至執委會，執委會得以施行法之方式，決定該行為守則於歐盟內具有一般規範效力，個資保護委員會應將所有經核准之行為守則登錄並以適當方式公開。

為確保企業遵循行為守則，得由經監管機關認證之機構予以監督，該機構有權於企業違反行為守則時將其停權或除名，該機構應具備之要件包括：獨立性、專業性、評估及審查程序、申訴程序與組織、無利害衝突等。

（四）認證⁸

GDPR 鼓勵建立個資保護認證制度，證明控管者及受託處理者之處理活動已遵行 GDPR，並應考量中小微型企業之相關需求。認證適用於國際傳輸時，控管者或受託處理者應透過契約或其他具有法律拘束力之文書，做成具有拘束力且可得執行之承諾，及適用該等適當之保護措施。認證應係自願申請，並透過透明程序取得，最長期限為 3 年，如符合規定者得更新。認證包括由經核准之認證機構或個資保護委員會所核准之標準與標章。

⁸ 詳參 GDPR 第 42、43 條。

認證機構應通過監管機關之認證，該認證機構須符合之要件包括：對所涉及認證事件具獨立性及專業性、遵守法定認證標準、建立資料保護認證程序、標章之核准、審查及撤回程序、申訴程序、無利害衝突等，監管機關對認證機構之認證最長期限為 5 年，並得於符合規定時更新。監管機關應將認證機構須符合之要件及標準公開，並送至個資保護委員會，個資保護委員會應登錄所有個資保護認證機制與個資保護標章，並以適當方式公開。

四、其他特殊例外情形⁹

於未取得前述適足性認定或未採行前述適當保護措施之情形下，欲將歐洲經濟區個資傳輸至其他第三國或國際組織時，GDPR 訂有相關特殊例外情形，適用上應從嚴解釋，僅於偶發與非重複性之傳輸時始得為之¹⁰。

相關特殊例外情形包括：個資當事人於接獲該傳輸對其可能造成風險之通知後，為明確同意者；該傳輸係為履行個資當事人與控管者間契約所必要者，或該傳輸係依個資當事人要求而為履約前所必要者；該傳輸對締結或履行控管者與其他人間基於個資當事人利益之契約所必要者；為公共利益之重要原因之必要傳輸；傳輸對建構、行使或防禦法律上之請求為必要者；於個資當事人身體上或法律上無法為同意之表示時，為保護個資當事人之重要利益之必要傳輸；傳輸係依據歐盟法或會員國法之特定公眾諮商目的者。

⁹ 詳參 GDPR 第 49 條。

¹⁰ Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, Adopted on 25 May 2018, 第 4 頁。

貳、GDPR適足性認定

GDPR 在國際傳輸規定中，由國家取得歐盟適足性認定者，則該國與歐盟間個資即可自由傳輸。目前已有 12 個國家或地區取得歐盟執委會之適足性認定¹¹，我國鄰近之日本與韓國亦積極與歐盟洽談適足性認定事宜，日本可望於今年秋季取得適足性認定¹²。

以下依據歐盟公布之適足性參考文件¹³，分別說明適足性概念、適足性認定程序、適足性評估要項等。

一、適足性概念

適足性的概念在歐盟 1995 年個人資料保護指令已存在，要求歐盟個資傳輸至第三國時必須確保該國符合適足保護程度（an adequacy level of protection），此概念經歐盟法院多次闡述，在 2015 年 Shremes 案確立一項重要標準，即第三國對於個資保護程度必須確保與歐盟實質相當（essentially equivalent），縱使雙方對於個資保護採取不同措施，最終若能達到相同的保護水準，第三國便具備適足性。由此可知，適足性評估雖可由法規對於當事人權利、個資控管者、受託處理者之義務，以及獨立機關監管之具備加以觀察，惟是否達適足保護之關鍵仍在於法規實際遵循程度以及執行效果，故在評估過程中，規範內容與執行手段同等重要，歐盟執委會對於實際執行效力將定期審核。

¹¹ 安道爾、阿根廷、加拿大（商業組織）、法羅群島、格恩西島、以色列、馬恩島、澤西島、紐西蘭、瑞士、烏拉圭，及美國（隱私盾）。

¹² http://europa.eu/rapid/press-release_IP-18-4501_en.htm

¹³ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

二、適足性認定程序

適足性認定程序係由第三國主動發起，歐盟執委會將對第三國法制規範及執行情形進行調查，並由其內部獨立專家提出評估報告，將相關資料及調查結果送請資料保護委員會提供意見，最終由歐盟國家代表批准該第三國是否具備適足性。依 GDPR 規定，歐盟執委會應定期對已取得適足性之國家進行評估，原則為至少每 4 年進行 1 次，另歐盟執委會有權撤銷、修正或暫停已取得之適足性認定，因此適足性認定之取得並非「終身制」，取得適足性認定之國家仍應持續保持自身個資保護法制水準與歐盟相當。

三、適足性評估要項

適足性評估要項包括第三國個資保護法制之基本原則、執行與程序機制、基於執法與國家安全對基本權利干預之限制等。

(一) 個資保護原則 (General Data Protection Principles)

1. 基本概念

第三國個資法規必須具備個資保護基本概念或原則，這些概念或原則雖無需複製 GDPR 用語，但必須反映並符合歐盟個資保護法規所載的概念，例如：個人資料定義、個資處理、資料控管者、資料受託處理者、接受者與特種個資等。

2. 合法、公平、合理之方式處理個人資料

個資處理應以合法、公平且合理之方式為之，應充分明確規範合法、公平及合理處理個資之方式。GDPR 之個資處理合理理由包括法律規定、個資當事人同意、為履行契約、為資料控管者或第三人之合理利益且該利益並未逾越個資當事人之利益等。

3. 目的拘束原則

個資之處理應基於特定目的，且不得為目的外之利用。

4. 個人資料品質之確保與比例原則

保有之個資應維持其正確性，必要時並應持續更新。個資之處理應適當、並與處理目的相關且不得逾越該處理目的。

5. 限制個人資料保存期間原則

原則上保有個資的期限不得逾處理目的所需之期間。

6. 個人資料安全與保密原則

於處理個資時，應確認該個資係以確保個資安全之方式處理，包括採取適當技術性或組織性措施，防止未經授權或非法處理個資、或使個資意外滅失、毀損或損害。安全措施等級之選擇應將當前最新技術與相關成本納入考量。

7. 透明原則

為確保公平，應以清楚、易於取得、簡明、透明及易懂之方式，告知個別當事人處理其個資之所有事項，相關資訊應包括：處理目的、資料控管者之身分、當事人可行使之權利與現有可確保公平性之其他資訊等。於部分情形下，如 GDPR 第 23 條所列之基於保障刑事偵查、國家安全、司法獨立、司法程序或其他與公眾利益相關之重大目的等情形下，可豁免此義務。

8. 個資當事人權利

個資當事人應有權確認其個資蒐集之處理情形，包括取得一份所有關於其個資被處理情形之副本。個資當事人於特定情況下應有權適當地更正其個資，例如該個資錯誤或不完整，以及於無必要處理其個資或非法處理其個資之情況下，請求刪除其個資。

個資當事人基於特殊情況下之合理理由，應有權隨時拒絕第三國依其法規所定要件，對其個資之處理，於 GDPR 包括因公共利益或執行職務之必要，或為資料控管者或第三人之正當利益之目的，而有處理該個資之情形，個資當事人得行使拒絕權。

個資當事人行使相關權利之程序不宜過於繁瑣。行使這些權利之限制，包括維護刑事偵查、國家安全、司法獨立及司法程序或其他如 GDPR 第 23 條之一般公共利益重要目的等情形。倘第三國有對於個資可攜權及限制處理權之規定，將有加分作用。

9. 國際傳輸限制

個資由原接收者為國際傳輸時，僅得於再接收者亦符合個資保護適足性之相關規定（或以契約約定），且該再接收者於處理個資時，須遵循個資控管者之相關指示時，始得為之。對於個資再為國際傳輸時，對原個資當事人之保護程度不應因再傳輸而降低。原自歐盟接收個資之接收者對於再接收者係處於未取得適足性認定國家之情形，應有責任確保再接收者已對個資提供適當保護。此種再傳輸個資僅限符合特定目的且具合法理由的情況下，始得為之。

10. 特種個資之保護

對於特種個資應有特定保護措施，GDPR 之特種個資係指第 9 條（種族或人種、政治意見、宗教或哲學信仰、工會會員之個人資料、基因資料、用以識別自然人之生物特徵識別資料、與健康相關或自然人之性生活或性傾向等資料）及第 10 條（前科犯罪資料）之相關個資。特種個資之保護應透過更多的個資處理要件予以落實，例如個資當事人對該處理應有明確同意或透過其他之安全措施予以確保。

11. 拒絕行銷權

個資當事人應有權隨時、且無須支付任何費用，拒絕以行銷為目的之個資處理。

12. 自動化決策及剖析

基於自動處理（包括剖析¹⁴），而對個資當事人產生具有法定效力或重大影響之決定時，僅於符合該第三國法規之特定要件時始得為之。依 GDPR，這些要件包括：取得個資當事人明確同意或為契約成立之必要。若該決定未遵循該第三國法規之特定要件，個資當事人有權不受其拘束，第三國法規並應提供必要之保障措施，包括：取得關於該決定所依據之具體原因和相關邏輯、得更正不精確或不完整之資訊、得就依據不正確事實所做出之決定提出異議。

¹⁴ 係指對個人資料任何形式之自動化運用，包含使用個資評估當事人其個人特徵，或分析、預測其工作表現、經濟狀況、健康、個人偏好、興趣、可信度、行為、地點或動向等特徵（GDPR 立法第 4 條第 4 款參照）。

(二) 程序與執行機制

1. 適當的獨立監管機關

第三國須設置一個以上之獨立監管機關，負責監管、確保並執行該第三國應具備之個資保護與隱私相關法規，該監管機關應完全獨立、公正行使職權，不受任何指揮。因此該監管機關應具備所有必備之權力與職責，以確保遵循個資保護權並促進對該權利之認知。該監管機關應編制人員和預算，且應具備主動調查權。

2. 個人資料保護機制須確保合規性

第三國應確保其個資保護機制具備高度的課責性，且確保個資控管者與受託處理個資人員皆知悉其應盡之義務與應負之責任，個資當事人亦知悉其權利及行使權利之方式。此外，應具備有效及具嚇阻性裁罰，以及可由相關機關直接驗證之機制，以確保法規之遵循。

3. 課責機制

第三國之個資保護架構應責成個資控管者與個資處理人員遵循相關規範，且得以向適當的監管機關展現其合規性。其方式可包括：個資保護影響評估、文件紀錄保存、相當期間內之個資處理紀錄、指定個資保護長或個資保護之設計與預設。

4. 當事人行使權利及救濟機制

當事人得請求合法救濟以迅速、有效、低成本地行使其權利，並確保法規遵循，爰應設置監管機制就相關申訴進行獨立調查，並使任何侵害個資保護權及未尊重隱私之行為皆被識別及處罰。當法規未被遵循時，應提供個資當事人有效的行政與司法救濟，包括因非法處理其個

資所致之損害賠償，並須具備獨立裁決或仲裁之制度，確保當事人獲得賠償，侵害者亦獲得適當裁罰。

(三) 第三國基於執法和國家安全對於基本權利干預之限制

有關將「第三國基於執法和國家安全對於基本權利干預之限制」納入適足性評估之考量，係源自歐盟法院 2015 年 Schrems 案之判決，爰本節先就 Schrems 案判決之重點摘要，再說明適足性評估時應考量之相關項目。

1. 歐盟法院 Schrems 案判決摘要

(1) 本案事實

A. 奧地利人 Schrems 自 2008 年起為臉書之用戶。任何欲使用臉書的歐盟居民，於註冊時即應與臉書愛爾蘭分公司訂定契約，允許其部分或全部之個人資料，傳送至位於美國的臉書總公司，並在總公司進行處理。

B. 2013 年 6 月 25 日 Schrems 向愛爾蘭個資保護機關申訴，請求禁止愛爾蘭分公司傳送其個人資料至美國，並以愛德華·史諾登為例，主張美國的法律和實務，並無法限制監控機關（如美國國家安全局（NSA）或 FBI）使用其個資。但愛爾蘭個資保護機關認為 Schrems 無法證明其個資遭 NSA 使用、且美國已被認定具有適足性，因此駁回其申訴。

C. Schrems 因此向愛爾蘭高等法院提起訴訟，法院認為雖電子監控或截取個資，係為公共利益之必要，但從愛德華·史諾登所揭露的事項看來，NSA 之行為已經過當。此種大量和無差別地

的獲取個人資料，顯然違反比例原則及愛爾蘭憲法所保障之基本價值。

D. 但因本案涉及歐盟對於美國安全港協議具備適足性之認定，應依歐盟法規定之相關程序進行檢視，因此法院決定停止訴訟程序，並提交予歐盟法院作初步裁決。

(2) 判決要旨

A. 「適當的保護程度」並非要求第三國應與歐盟法規所訂之保護程度「相同」，而是指第三國應確保其國內法或國際承諾，對於基本權與自由的保護，與歐盟 1995 年個人資料保護指令及歐盟基本權利憲章實質相當；且因第三國的保護程度可能發生變化，因此歐盟執委會應定期檢視。

B. 第三國是否具備適當保護程度，係由歐盟執委會決定，即便該第三國與歐盟的保護方式不同，但只要能確保他保護的方式與歐盟實質相當即可。

C. 保護個資是為了尊重私人生活的基本權利，若將個資傳輸至第三國，但卻未能確保該第三國具有適當的保護程度，將會有大量人民之基本權利受到侵害。因此，當歐盟執委會檢視第三國是否具有適當保護程度時，依歐盟 1995 年個人資料保護指令及歐盟基本權利憲章，應予嚴格認定。

D. 依據歐美安全港協議，只要美國的企業、組織遵循安全港原則及美國商務部所訂之相關文件，則認定該企業、組織具備跨境傳輸之適當保護程度。但安全港原則僅適用於自願參與安全港認證之美國企業或組織，美國政府機關無需遵守。

- E. 又依據歐盟該項決定，美國基於國家安全、公共利益之理由或依其國內立法，即得干涉自歐盟傳輸至美國之個資基本權，但此項行為已造成對私人生活基本權利之影響。
- F. 美國政府機關能查閱自歐盟傳輸之個資，並以與歐盟不相當之保護方式處理該資料，已超出國家安全保護之必要性及範圍。此外，美國亦未賦予當事人行政或司法救濟管道（特別是請求更正或刪除其被查閱的資料之權）。
- G. 歐盟認為，僅於絕對必要的情況下，始能排除及限制個資保護；對於以自動化方式處理個資，或具有非法取得個資之重大風險者，應增加相關保護措施。
- H. 歐盟執委會依 1995 年個人資料保護指令第 25 條關於適當保護程度所作成之決定，應明確說明該第三國國內法或所簽署之國際承諾，確與歐盟之基本權利保護程度相當，但執委會於歐美安全港協議，卻並未說明美國之國內法或國際承諾是否已確實達到適當保護程度。
- I. 因此，歐美安全港協議因不符合歐盟 1995 年個人資料保護指令及歐盟基本權利憲章而無效。

2. 評估要項

依 GDPR 第 45 條第 2 項第 (a) 款規定，歐盟執委會進行適足性評估時，應考量一般及各個部門的相關法規，包含涉及公共安全、國防、國家安全及刑法，以及公務機關取得個資與相關法規的執行面。

第三國基於執法和國家安全目的而對基本權利干預應遵循 4 項原則¹⁵：

¹⁵ Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).

(1) 個人資料處理應基於明確且公開之法律依據

政府干預手段必須依法為之，且該法律內容應具有可預見性。法律除須正確、清楚以及公開外，亦應明文規定得進行資訊監察及監控的違法行為性質、被監控者的類型、期間限制、對取得資料檢視、使用和儲存應遵行的程序，以及與其他單位進行資料傳輸的預防措施，也包括主管機關資料取得的情形與實體及程序性條件。另針對通訊監察之許可條件及明確性的規範，亦應適用相同之原則，而無另定其他標準之理由。

誠然，可預見性無法適用於各種狀況，如通訊監察具有其隱密性，公權力若要取得某人的通訊資訊，所謂可預見性之要求不代表當事人應可以預知有關機關何時將進行通訊監察，進而有所因應。但考量恣意濫權的風險，因此訂定一套清楚、詳細的電話監聽規範至為重要。尤其在科技日益發達的情況下，法律應該清楚明白告知人民，在什麼樣的情況下，公權力可能會採取的措施。

(2) 合目的之必要性及合目的性

國家機關對個資之處理，均構成對於隱私及資料保護之干預，即使是為情報蒐集之目的而處理個資，也只在達成合法目的所必要，符合比例原則之情形下，始具有正當性。

依據歐盟法院判決，一般性、普遍無差別之通信資料儲存要求，將抵觸 E-Privacy Directive (2002/58/EC) 及歐盟基本權利憲章之規定。至於有關通信內容之資料，歐盟法院在 Schrems 案中明確指出，公權力不得基於一般性之理由存取。

(3) 個人資料之處理應受獨立監管

依據歐洲人權法院判決之意旨，獨立監管應該及於整個資料運作的週期，包括開始授權監控、執行及結案等階段。另考量為情報

蒐集目的處理個資之特殊性，特別是在開始監控及執行兩個階段，允許在當事人未知之情況下處理其資料；鑑於在此情境下，個案濫權之情形非常容易發生，甚至可能對民主社會造成傷害，因此將監管權交由法官行使即非常必要，司法機關可以確保在獨立、公平及適合程序下進行監管。

此外，歐盟法院亦指出，存取先前儲存之資料須經法院或獨立行政機關事前審查；這些審查機關所為之決定，應在有關機關遵循預防、偵查或刑事訴追之程序提出合理之請求後為之，並應將資料之存取及利用，限於達成特定目的所必要之範圍。

關於事後之監管，則與個人之救濟有關。值得注意的是，在某些情況下，也可能由有關機關依據職權，進行事後監管，以確認監控措施確實符合法令。

關於獨立之監管機制，歐洲人權法院表示其屬意由法官為之。但是，此並非排除得由其他機關作為監管機關，只要該機關能獨立於政府行政權之外，且有足夠權力執行監管職務即可。至於評估監管機關是否獨立，歐洲人權法院曾表示，其成員之任命方式與法定地位應納入考量。例如，成員具有司法人員之任用資格，且由國會或總理任命，即具一定獨立性。相對地，內政部長係政治任命，且直接參與監控業務，因此不具有獨立性。此外，歐洲人權法院也強調監管機關審查時，必須能夠接觸所有必要文件（包括密件），且監管機關本身之作為是否受到公眾檢視，也是考量因素之一。

(4) 應予個資當事人有效之救濟

歐盟基本權利憲章規定，當人民就歐盟法律保障之權利遭受侵害時，應有向法院或其他審理機關（構）請求有效救濟之權利。在基於執法或國家安全目的對人民進行監控之情形，歐洲人權法院認為，有效救濟之問題，與監控結束後是否通知當事人相關監控措施息息相關；因為監控是在人民不知情之情況進行，除非當事人於事後獲得通知，或是於懷疑自己遭到監控時即向法院提起訴訟，人民才有機會去挑戰該監控行為之合法性。歐洲人權法院亦認為，如未建立事後通知之機制，在符合以下標準之情況下，也可以認為提供有效救濟：由司法人員或具經驗之律師組成之獨立公正機關（構），依據相關程序，針對人民提出之異議進行審查，並有權調閱相關資料，且得對違法行為作成救濟之決定。

叁、小結

GDPR 就個資之國際傳輸規定包括第三國或國際組織取得歐盟執委會之適足性認定、由企業自主採行符合 GDPR 規定的適當保護措施、其他特殊例外情形等。

由國家取得適足性認定部分，我國今年 5 月底已由國發會正式向歐盟表達我國申請適足性之意願，目前國發會刻就適足性認定所需資料積極整備，並與相關部會及專家學者密集研商，期能與歐盟儘速展開適足性認定之技術性對話。在尚未取得適足性認定前，企業應依 GDPR 規定自主採行適當保護措施，於少量、非經常性之國際傳輸情形，則可採用相關特殊例外情形之規定為之。🌀



名家 觀點

VIEWPOINT

GDPR與數位經濟 ——歐盟的企圖與啟發

理律法律事務所 曾更瑩律師

壹、前言

貳、歐盟對於個資保護以及數位經濟發展之企圖 與布局

參、GDPR 給予數位經濟發展之空間

肆、結語

壹、前言

數位經濟在近年之發展突飛猛進，電腦運算能力之增強、行動裝置之普及、網際網路連線能力與速度之進步，帶動新科技之開發與誕生，商業模式之創新與蓬勃發展。社群網站、通訊軟體被廣泛使用，其型態從早期的部落格、微博、臉書（Facebook）、到近期的 Line，將社群網站、即時通訊之功能開發到極致，之後又有其他吸引年輕族群的社交媒體竄起；影音串流技術進步，如今在各大 OTT 網站上放映的影片，品質不輸傳統電視甚至青出於藍，各種直播、短視頻平台也在世界各地頭角崢嶸；

Uber、Airbnb 等「共享經濟」、「平台經濟」迫使傳統既得利益業者反思與進步，也使大家重新思考與反省傳統管制經濟之方式與內容是否合理；在中國崛起的電子支付、第三方支付等工具，在世界各國包括臺灣，還在摸索與考量是否全盤接受之時，虛擬貨幣、加密貨幣和形形色色的 ICO 已經對全球之金融監理機關拋出一道道難解的習題，而其所奠基之區塊鏈技術也在各行各業發展出各種應用；在軟、硬體技術進步，海量資料之蒐集與分析成為可能後，機器學習、人工智慧之急速發展彷彿即將使科幻小說中的場景化為現實，如果此番人工智慧之泡沫在最近持久不消，人工智慧之發展更有可能顛覆目前所有數位經濟之模式與人類未來生活之圖像。

凡此種種，追根究底，「資料」之蒐集、分析、利用，是數位經濟發展背後極為重要的動力，也是上述諸多科技發展與商業模式得以扎根、茁壯的沃土。掌握資料來源、開發創新思維、加上精確分析資料之科學能力，將是未來發展數位經濟的關鍵。然「資料」之蒐集與分析成果之誕生，與「個人資料」和「隱私」密不可分，過往數位經濟發展之模式，大多數奠基於大量「使用者」個人資料與行為模式之分析，進而產生對於隱私以及人權保護不周之疑慮，而有心人士對於個人資料之誤用甚至濫用，亦造成公眾之紛擾與不樂見之後果。是以「個人資料」之保護與數位經濟之發展間應如何調適與平衡，當為現今重要課題。

歐盟的一般資料保護規則（General Data Protection Regulation, GDPR）在今（2018）年 5 月 25 日生效，因為涉及域外效力和高額行政罰

款，對全世界投下不小之震撼彈。在 GDPR 如此重裝備戒護個人資料之下，歐盟將如何調適個人資料之保護與數位經濟之發展？本文茲分享個人觀察心得。

貳、歐盟對於個資保護以及數位經濟發展之企圖與布局

一、美歐個資保護大不同

歐盟各國為世界立法例中，制定完整個人資料保護法典之先驅。在歐盟，個人資料以及隱私之保護，被視為人權之內涵，高規格保護之。而在大西洋對岸的美國，並無全國統一適用之個人資料保護法典，對於個人資料及隱私權保護之法律散見於各州法規中，加上矽谷新創企業強勁旺盛的爆發力，在數位經濟發展之浪潮中不斷拔得頭籌，一路領先全球。歐盟對於美國鬆散之隱私管制方式一直無法認同，過去兩地曾以「安全港」之方式允許歐盟之個人資料被傳輸至美國，在 GDPR 生效後，亦持續討論以「隱私盾」方式允許歐盟境內之自然人之個人資料得以傳輸至美國。

歐盟與美國之間對於個人資料以及隱私權保護之歧見，當以歐盟與 Internet Corporation for Assigned Names and Numbers（網際網路名稱與數字位址分配機構，簡稱「ICANN」）之間就 ICANN 的「WHOIS」資料庫之改良與存廢之大戰為著例之一。ICANN 是在美國商務部主導下，負責全球網域名稱與位址之分配之非營利公司法人，ICANN 的 WHOIS 資料庫歷史由

來已久，為便利各網站之管理人員彼此連繫，WHOIS 資料庫中存有不少個人資料，方便公眾查詢。多年以來歐盟多次質疑 ICANN 的 WHOIS 資料庫存放或公開過多不必要之個人資料，對於個人資料以及隱私保護不周；從 GDPR 立法至生效，特別是在今年 GDPR 生效前夕，ICANN 與歐盟雙方數度交火，ICANN 甚至在 GDPR 生效當日立即在德國法院提出假處分聲請，企圖得到法律上之支持，取得繼續與歐盟作戰之時間與空間；惟德國法院在很短時間內即駁回 ICANN 的聲請，拒絕為 ICANN 背書。美歐兩地自由開放與嚴密保護兩股勢力之歧異與角力可見一斑。

二、GDPR對於數位經濟之宣示

歐盟 GDPR 如此高規格保護個人資料，難道不擔心扼殺其本土境內原本已經落後美國的數位經濟？在 GDPR 生效之後，歐盟本土網站亦有被迫關閉停止營業者，例如英國的工具共享平台 StreetLend，原先係一以倫敦為主要服務區域，為便利鄰居、朋友分享借用家中閒置不用的工具之平台，例如家中如有平常使用機率不高的梯子、螺絲起子或電鑽等，均可加入分享之行列。在 2018 年 4 月，GDPR 正式生效以前，StreetLend 即在其官網上宣布因為 GDPR 造成之不確定性與風險，加上違法之高額罰款，使其不得不宣布停止營業。GDPR 之威力可見一般，尤其係對於新創與中小企業之影響甚為顯著。

然 GDPR 果真忽視數位經濟發展，棄新創與中小企業於不顧？實則 GDPR 前言揭示諸多上位原則與精神，顯示 GDPR 之目標包含促進個人資料自由流通以及建立消費者信任等，亦透露促進數位經濟之發展實為歐盟未來之目標之一，而 GDPR 之實施與生效乃為其一手段。

GDPR 前言第 5 點，表示歐盟內部市場之功能，所帶來的經濟與社會之整合，造成個人資料跨境流通之實質增加；公部門與私部門間對於個人資料之交換，包含歐盟境內之自然人、協會、組織之間之資料交換，業已增加。歐盟呼籲成員國之中央主管機關間應相互合作，以便協助彼此履行有關任務。GDPR 前言第 6 點，表示科技之快速發展與全球化之進程對於個人資料保護帶來新的挑戰，個人資料蒐集與分享之規模與幅度大為增加，科技使得公、私部門均得以史無前例之幅度使用個人資料以從事相關活動。自然人不斷允許其個人資料為公部門以及私部門所蒐集、利用，科技已使經濟與社交生活轉型，是以應進一步「促進」(facilitate) 個人資料於歐盟境內之自由流動，以及向第三國以及國際組織之自由流動，並同時確保對於個人資料高規格之保護。以上種種，表示歐盟亦了解在現今科技發展與經濟環境下，個人資料大量被蒐集與利用之現實，也肯認在此發展趨勢與環境之下，個人資料自由流動有其必要，惟歐盟同時亦強調對於個人資料需要高規格之保護。

GDPR 前言第 7 點，表示為建立數位經濟在歐盟內部市場之發展，建立「信任」十分重要，基此，有關發展需要歐盟建立堅強且更為一致之個資保護架構，該架構必須奠基於強力執法。自然人應被賦予對其自身之個人資料之

掌控權，法規面以及實務面對於自然人、業者以及主管機關之確定性應被加強。GDPR 前言第 9 點則指出雖然過去歐盟個人資料保護指令之立意甚佳，惟未能避免歐盟成員國在執行個人資料保護法規之分歧，造成法律之不確定性，也造成公眾認知在個人從事網路活動時，對於自然人之保護存有相當大之風險，是以，歐盟認為在歐盟境內之成員國若對於個人資料之保護彼此之間存有歧異，將大為阻礙個人資料在歐盟境內之自由流通，造成歐盟經濟活動發展之障礙，扭曲競爭，也妨礙各國主管機關履行其職務。GDPR 前言第 10 點則繼續強調，為達成一致且高標準之個人資料保護，移除個人資料在歐盟境內自由流動之障礙，歐盟成員國應對於個人資料之保護採取統一且一致性之規則制定與解釋；GDPR 前言第 11 點更強調，在歐盟境內對於個人資料有效之保護，端視各國對於違反個人資料法規之制裁與執行採取一致性之強度與密度；GDPR 前言第 13 點亦闡述，為確保在歐盟境內對於自然人之保護程度之一致，避免彼此之間之歧異造成個人資料之自由流動之阻礙，GDPR 之規範對於不論大小之業者，含微型企業、中小企業等，均應具有法律上之確定性且應透明，對於歐盟境內之自然人提供相同程度且法律上具有執行力之權利，同時各成員國之主管機關應採取一致性之執法力度並彼此合作。為此，GDPR 對於員工人數少於 250 人之企業採取法規部分鬆綁，也鼓勵成員國在適用 GDPR 時對於微型企業以及中小企業作不同考量。

以上載於 GDPR 前言之宣言，顯示歐盟亦有發展數位經濟之共識與決心，但是歐盟認為數位經濟之發展必須以完善之個人資料保護為前提，於此

前提，取得消費者之「信任」十分重要，惟有維持歐盟對於個人資料保護之高標準始有可能建立「信任」；而歐盟成員國彼此之間若對於個人資料之保護採取之標準不一，執法程度嚴峻、寬鬆不同，將不利個人資料在成員國間之自由流動，連帶阻礙歐盟整體數位經濟之發展與市場競爭。是以，歐盟利用 GDPR 統一（或強迫）其成員國對於個人資料保護之程度與執法力度，乃著眼於促進其境內個人資料之自由流動，同時希望個人資料之自由流動能進一步帶動歐盟整體數位經濟之發展，不可不謂用心良苦。在今年臉書（Facebook）與劍橋分析（Cambridge Analytica）爆出個人資料遭濫用之事件後，世人對於個人資料之保護更為重視，也開始對於過去以「隱私」換「便利」之網路使用型態以及「免付費」數位經濟之發展模式加以反思，GDPR 所要求之諸多法規遵循措施正好可用以重建「信任」，而 GDPR 之域外效力也使 GDPR 不但成為全球各地有識之士共同閱讀與理解之法律文件，其中諸多原則也成為評斷個人資料保護是否周全之標準。是以雖然 GDPR 陳義甚高，法律遵循義務十分繁重，連歐盟境內之企業也大嘆吃不消，其中所揭示之基本原則儼然已成為檢視對於人權保護之程度與方式某種意義上之普世基準。

三、歐盟擬促進「非屬個人資料之資訊」之自由流通

在制定 GDPR 之同時，歐盟內部也在討論另外一套法案，亦即對於「非屬個人資料之資訊在歐盟境內自由流動之架構」（Regulation of the European Parliament and of the Council on a framework for the free flow of non-

personal data in the European Union)，此草案於 2017 年 9 月間提出討論。該草案之提案說明開宗明義即提到新型數位科技、例如雲端運算、大數據、人工智慧、物聯網等等，都是為了能夠增進使用者靈活度、生產力、速度與自治能力之工具；歐盟之數據市場預估在 2016 年至少有六千億歐元的產值，與 2015 年相比成長 9.5%，而根據歐盟之研究，歐盟之數據市場到 2020 年時有成長到超過一兆零六十億歐元之潛力；而為了將此潛力化為可能，歐盟提案意在處理下列問題：

- (一) 改進歐盟單一市場境內因各成員國資料在地化 (data localization) 要求所形成之非屬個人資料之資訊之流通障礙；
- (二) 確保主管機關於執法時取得資料之權力不受阻礙；
- (三) 確保資料之專業使用者能在不同之資料儲存處理服務提供者之間自由轉換，同時不對服務提供者造成多餘之負擔或因而扭曲市場。

歐盟之目標係達成更具競爭力、統整之資料儲存、處理之內部市場。為達非屬個人資料之資訊得以在歐盟境內自由流通之目標，歐盟在提出上述法規草案之時，不僅進行相關研究，亦徵詢公共意見 (public consultation)、進行影響評估 (impact assessment) 等等。

該草案文字在一開始提到，隨著經濟數位化之加速，資通訊科技 (Information and Communications Technology, ICT) 已不再係單獨之領域，而係所有現代創新經濟與社會體系之基礎。電子資訊是該體系之中心，當分

析電子資訊或將電子資訊與服務以及產品結合之時，將產生更大之效益。資料之價值鏈建立在不同之資料相關活動上，包括資料之生成、蒐集、彙總、組織、儲存、處理、分析、行銷、分銷、利用與再利用等活動。資料價值鏈之建立奠基於有效果並有效率之資料儲存與處理功能；然而，在歐盟單一市場境內，有效果與有效率之資料儲存與處理功能、以及資料經濟之發展為兩種對於資料流通性以及單一市場之障礙所阻撓。其一為歐盟成員國內國法下之「資料在地化」之法令要求；其二則為私人之間在法律上、合約上以及技術上對於更換資料儲存或處理服務提供者所形成之障礙。因此，為求法規明確化以及提供公平競爭之環境，為歐盟內部市場所有相關參與者訂定統一之規範乃為關鍵。

草案第 4 條要求成員國不得限制資料之儲存或處理必須限定位於某一成員國境內；除非為了公共安全之考量，資料之儲存與處理在任一成員國都不得被禁止或限制；成員國若有「資料在地化」之立法，應於草案生效後十二個月內廢除之。草案第 5 條規定，各主管機關依照歐盟法或各成員國法下之規定行使職權要求資訊提供之權力，不可因此受到影響；主管機關查詢資料之要求或命令，不可以資料儲存在其他會員國為由而加以拒絕；如果某一成員國之主管機關業已窮盡各種可得之方法索取資料，但仍無法取得時，該成員國之主管機關得請求其他成員國之主管機關協助以取得資訊。草案第 6 條則要求歐盟鼓勵業者自律，訂定準則或最佳行為規範以方便使用者更換服務

商，以便專業之資訊使用者能在獲取更充分、詳細、透明之資訊之前提下，與資料儲存與處理之業者簽訂服務契約。草案第 7 條則要求各成員國就草案所規範之事項設置單一連繫窗口以促進未來成員國之間以及與歐盟之間就相關事宜之溝通。

觀察上述草案，雖然該草案著眼於歐盟單一市場之整合，希望透過去除成員國間之法規壁壘等方式，加大歐盟內部單一市場規模，強化歐盟在數位經濟之角色，增加歐盟在資訊市場之產值；惟該草案涉及「資料在地化」立法廢除、擴大主管機關向民營業者索取資料之權力、迫使民營業者便利其等之客戶互相轉換服務提供商，在歐盟境內整合之阻力勢必不小，未來該草案是否能順利在短時間內完成立法亦值得觀察。

然若將該草案與甫生效之 GDPR 綜合觀之，可知歐盟之企圖心不只在於建立「信任」、保護基本人權、提升歐盟境內之個人資料與人權保護，更在鞏固歐盟單一市場之地位，希望歐盟境內之自然人之個人資料能在高規格之保護下在歐盟境內自由流通，發展歐盟境內之數位經濟，同時也倡議「非屬個人資料之資訊」在歐盟境內自由流通，促進歐盟各成員國對於數位、資訊經濟之競爭，激發資訊與產品、服務間之加值效應，最終不僅係將歐盟建置為相較於世界其他各地而言，個人資料保護與人權保護較為完整、周全之數位經濟發展環境，亦希望資訊經濟、資料分析、處理、儲存等業者能在單一市場自由流通之環境下，發揮相輔相成之綜效。

叁、GDPR 給予數位經濟發展之空間

GDPR 加諸業者繁複之法遵義務，但亦有若干措施給予數位經濟某種程度之發展空間，茲試舉數例說明之：

一、匿名化（Anonymisation）與去連結化（Pseudonymisation）

（一）匿名化（Anonymisation）

承襲 GDPR 之前身，歐盟個人資料保護指令，對於「匿名化」資料之看法與見解，GDPR 在前言第 26 點明白宣示，個人資料保護之各項原則對於「匿名化」資料並不適用，而所謂「匿名化」資料意指與「已識別」或「可得識別」之個人無關之資料，或是經過匿名化處理而無法再藉以識別任何個資當事人（data subject）之資料，是以 GDPR 並不適用於匿名化資料之處理，包含為統計或為研究目的所為之處理。匿名化資料一方面並不適用 GDPR 之相關規範，得以自由處理與利用，另一方面，依照歐盟正在草擬之「非屬個人資料之資訊在歐盟境內自由流動之架構」，匿名化資料非屬個人資料，歐盟未來亦會致力於促進該等資料在歐盟單一市場內之流通。是以，如數位經濟業者能從「匿名化」之角度開發其業務，或許能降低其被控侵害他人個人資料或隱私之風險，亦能減少其在 GDPR 下之法遵尊義務。

然而，個人資料如何進行「匿名化」？資料科學家以及資訊工程師等均表示個人資料要完全「匿名化」在現實上幾乎不可能。「匿名化」之概念在 GDPR 誕生之前即幾經討論，歐盟 Article 29 Data Protection Working Party 在 2014 年 4 月 10 日提出關於「匿名技術之意見」（Opinion 05/2014）。此份「匿名技術之意見」對於個人資料之「匿名化」提示若干重點如下：

- 第一、個人資料是否已經完全匿名化，歐盟個人資料保護指令並未採取科學上絕對無法識別個人之標準，而係以經匿名化處理之個人資料，在日後是否於「合理」之情況下無法再被識別為準，同時亦需考量在「資料開放」政策風行之下，個人可能在低成本之情況下再為識別之可能性。此一概念試圖在進行「匿名化」之努力以及「再為識別」所可能花費之時間以及資源之間取得平衡。
- 第二、有效個人資料「匿名化」之標準包括三要素：(1) 並未挑出單一之個人 (no singling out of an individual)、(2) 經過「匿名化」處理之資料與個人有關之記錄不再有所連結 (no linkability between records relating to an individual)、(3) 無法自資料再推論出與某位個人相關 (no inference concerning an individual)。
- 第三、所謂「匿名化」係指對於資料控管者 (Data Controller) 以及對於其他任何人而言，均無從識別。若資料控管者以單一事件 (Event) 為單位分類資訊，以僅僅抹去個人之姓名或識別碼之方式進行匿名化，效果仍然有限，控管者必須先將資料彙整，僅提供經過彙整之後之資訊，始該當匿名化資訊。
- 第四、當第三方接收到經適當匿名化處理之資料之後，由於該等資料已經無法識別個人，第三方於利用與處理該等資料之時，無需再遵守個資保護相關原則。

第五、將所蒐集來之個人資料進行「匿名化」時，仍然屬於個人資料之「處理」之一種，資料控管者在進行「匿名化」時仍應考量「目的限制」，亦即個資當事人對於個人資料處理之合法期待，是以「匿名化」仍然必須在蒐集之原始目的範圍內為之。

此份「匿名技術之意見」同時對於目前已知之資料匿名化處理技術加以討論與著墨，對於某些技術之使用與弱點加以提點與建議。未來此份文件仍將是在 GDPR 架構下解釋「匿名化」資訊以及鑑別某項資料是否應被視為個人資料之重要參考依據。數位經濟發展如欲「擺脫」GDPR 沉重的法遵義務，應考量盡量蒐集與利用「匿名化」資訊。

(二) 去連結化 (Pseudonymisation)

GDPR 對於「去連結化」此一概念討論甚多，一般認為若資料控管者對於個人資料進行「去連結化」，將有助於其對 GDPR 各種要求之遵循。GDPR 第四條第五款將「去連結化」定義為將個人資料處理之後，使得該等個人資料在無其他額外資訊之協助比對之下，無法再歸屬至任何特定之個資當事人，而該等「額外資訊」必須與經「去連結化」處理後之資料分別保存，同時應有組織上與技術上之措施以確保該等資料無法再指向任何「已識別」或「可得識別」之個人。所謂「額外資訊」之保存可以加密方式為之，亦應考量限制可以閱覽、使用該等「額外資訊」之人員之人數。應注意的是，「去連結化」之資訊對於資料控管者來說仍然係個人資料，GDPR 各條款仍然對其適用。然若採行「去連結化」，對於 GDPR 之遵循，至少有下列益處，對於歐盟推動數位經濟亦有幫助：

第一、GDPR 第 6 條第 1 項 (f) 款，對於個人資料之合法處理事由，訂有將資料控管者以及個資當事人之利益加以權衡考量之所謂「正當權益」(legitimate interests) 之事由，亦即資料控管者可為其自身或第三人之「正當權益」處理個人資料，但需權衡個資當事人之利益、基本權利與自由，而僅得於資料控管者或第三人之「正當權益」不為個資當事人之利益、基本權利與自由所凌駕時，始得為之；特別係在個資當事人係孩童之情況下。GDPR 第 6 條第 4 項對於非基於個資當事人同意而處理個人資料時，訂有利益權衡之考量因素，其中 (e) 項即為適當安全措施之採行，該等安全措施包含「加密」以及「去連結化」。

第二、GDPR 第 25 條宣示從設計面保護個資以及個資保護應為原始設定之原則 (Data Protection by design and by default)，要求資料控管者在考量當時科技水平、實施之成本、個資處理之性質、範圍、情境、目的，以及對於個資處理對於自然人權利與自由可能造成之風險之下，在技術上與組織上採行適當之措施，以有效之方式將個人資料保護內建於處理程序之中。所謂之技術上與組織上適當之措施，其中之一即為對於所持有之個人資料「去連結化」。

第三、GDPR 第 32 條揭示保護個人資料安全之基本原則，要求資料控管者以及處理者在考量當時科技水平、實施之成本、個資處理之性質、範圍、情境、目的，以及對於個資處理對於自然人權利與自由可能造成之風險之下，在技術上與組織上採行適當之措施，以針對可能之風險保護個人資料之安全，其中，個人資料「去連結化」即為 GDPR 所舉出之技術上與組織上適當之措施之範例之一。

第四、GDPR 第 33 條要求資料控管者於知悉個人資料侵害事故時，最遲於 72 小時內通知歐盟之監管機關，除非資料控管者依照 GDPR 所訂定之相關原則能證明該個人資料侵害事故對於自然人之權益與自由並無風險。GDPR 第 34 條亦規定如該個人資料侵害事故對於自然人之權益與自由有可能造成風險時，資料控管者應立即通知個資當事人，而如資料控管者原已採行適當措施使所外洩之資料無從識別個資當事人時，該等通知義務得以豁免。若資料控管者於個資處理流程中採行「去連結化」措施，而所外洩之資料限於已「去連結化」之部分而不含得以重新識別當事人之資料時，資料控管者比較可能證明與主張個人資料侵害事故對於個資當事人之權益無影響或所外洩之資料無從識別個資當事人，而免除對於監管機關或個資當事人之通知義務。

二、取得當事人同意之方式

GDPR 第 13 條以及第 14 條要求資料控管者對於個資當事人所應履行之資訊揭露義務非常繁重，需告知個資當事人之資訊不但項目眾多，又要求告知個資當事人其等在 GDPR 規範下所享有之諸多權利，加上歐盟以及成員國各自之法律規定，合乎歐盟規定之個人資料告知事項 / 隱私權政策不僅無法將其要義「一言以蔽之」，也相信沒有任何一位非專業人士之個資當事人有耐性與能力一一讀完。

幸好，GDPR 在取得當事人同意之「形式」方面之要求，並未如對於資訊揭露之要求一般複雜；一來並未要求以書面為之，也不要要求以電子簽章或電子文件為之，如此數位經濟之業者可以利用在網頁上點選「同意鍵」方式取得當事人同意；二來在同意之實質內容上，並未要求資料控管者在取得當事人同意之前先對當事人諄諄教誨（要求個資當事人將冗長之個資資訊揭露事項讀完或對個資當事人口頭念一遍），只要將個資處理之目的講清楚、說明白，並告訴個資當事人其等有隨時撤回 / 撤銷個資同意之權利，即可取得有效之個資同意，至於冗長的個人資料告知事項 / 隱私權政策，只要提供網頁連結給個資當事人參考即可。此種取得同意之方式較為簡便，對於數位經濟業者來說較為容易遵循，也方便個資當事人對於個資蒐集之目的得以一目了然。

三、行使當事人權利之例外

GDPR 第 15 條至第 23 條，賦予個資當事人諸多基本權利，乃係本次 GDPR 傲視全球之亮點之一。該等當事人權利包括：個資當事人近閱權

(Right of access by the data subject)、更正權 (Right to rectification)、刪除權 / 被遺忘權 (Right to erasure/ right to be forgotten)、限制處理權 (Right to restriction of processing)、資料可攜權 (Right to data portability)、拒絕權 (Right to object)、對於個人之自動化決策與側寫 (Automated individual decision-making, including profiling)，對於個資當事人之保護十分周全綿密。

同時，GDPR 也鼓勵採取去連結化、加密或其他技術上或組織上之措施，以保護個人資料之安全，因此，企業在處理利用個資之過程中，很有可能已經將部分個人資料匿名化，而有再識別之困難。若此時個資當事人回過頭來要求行使上述個資當事人之權利，例如目前最著名之「被遺忘權」，難道資料控管者此時應該將已經除去識別資訊或匿名化之資訊再度識別，以方便個資當事人行使「被遺忘權」？若答案為肯定者，則不吝減低企業以匿名化方式處理個人資料之動力，亦提高數位經濟業者進行資料分析之成本與風險。

關於此，GDPR 第 11 條規定，於資料控管者處理個資之目的不再需要識別個資當事人之時，資料控管者並無義務僅僅為了遵循 GDPR 各種規範之目的，繼續保存、取得或處理額外得以用來識別該等個資當事人之資訊。此時，如有可能，資料控管者應將上情通知個資當事人。在此情形下，GDPR 第 15 條至第 20 條個資當事人之種種權利即不再適用，除非個資當事人自行提出額外資料以便得以再識別該名個資當事人。GDPR 前言第 57 點表示，若資料控管者所處理之個人資料並不允許資料控管者識別某一自然人，該資料控管者無庸為了遵循 GDPR 下之義務，另行取得額外資訊以資識別某一自然人；然而，若個資當事人主動提供相關之額外資訊，資料控管者亦不應拒絕

協助個資當事人進行再識別。有關之識別資訊包含數位識別，例如以過去個資當事人登入資料控管者所提供之線上服務所需之資訊等，作為識別之方式。

上述規定應係在「當事人權利之行使」，「資料控管者進行匿名化、去識別化所為之努力」，與「再識別所需耗費之成本與資源」等之間，所為之利益權衡，正好可以在數位經濟之發展，以及 GDPR 繁重之法律遵循義務之間，有所平衡與調適。

四、對於微型、中小企業之放寬措施

數位經濟之誕生與崛起，都會經過微型企業、中小企業這段過渡期，歐盟制定 GDPR，意圖對於微型企業、中小企業，提供較為寬鬆之法律管制。GDPR 前言第 167 點要求歐盟執委會在行使 GDPR 所賦予之權力時，應考量針對微型企業以及中小企業採取特定之措施。GDPR 第 40 條要求成員國、監管機關、歐盟執委會等應鼓勵建立為適用 GDPR 之行為規範（Code of Conduct），並要求其等考量微型企業以及中小企業之特殊需求。GDPR 第 42 條要求成員國、監管機關、歐盟執委會等應鼓勵個人資料保護認證措施之建立，特別是在整個歐盟之層次上，考慮建立該等認證措施，包含個人資料保護標章等等，而在建立相關認證措施時，GDPR 亦要求對於微型企業以及中小企業之特殊需求加以考量。

除了在執法層面以及在行為規範、認證措施等面向考量微型企業以及中小企業之特殊需求以外，GDPR 具體豁免微型企業以及中小企業之法律遵循義務，在於以員工人數是否達到 250 人為標準，決定一企業是否應該依照

GDPR 第 30 條規定，對於企業之個人資料處理活動保留紀錄。GDPR 第 30 條對於企業處理個人資料所應保留之活動記錄訂有詳細的規定與要求，為符合該條規定，企業必須為其處理個人資料之活動保留下列資訊：

- (一) 資料控管者之姓名以及連絡方式；
- (二) 處理資料之目的；
- (三) 個資當事人之類別以及個人資料之類別；
- (四) 個資被揭露之對象之類別，含位於第三國者或國際組織；
- (五) 個資傳輸至第三國或國際組織者，第三國或國際組織之名稱，依 GDPR 所要求採取的適當保護措施相關之文件；
- (六) 各種不同類別之資料預計可能之刪除時限；
- (七) 依 GDPR 所要求採取的技術上與組織上之措施之簡述。新創企業之員工人數應遠低於 250 人，得以豁免上述繁複之記錄義務，可節省不少資源，集中力量發展數位經濟。

肆、結語

綜上所述，GDPR 闡述與擘劃對於個人資料、隱私、人權保護之崇高藍圖，畢竟「科技始終來自人性」，來自於個人者終將回歸至個人，能取得個人之信任與信賴，數位經濟才有沃土繼續茁壯成長，若任由個人資料或隱私遭到濫用，可能造成意想不到之後果，不可不慎。歐盟在利用 GDPR 提高個人

資料保護水準並統一成員國間對於個人資料保護制度與法規之歧異之同時，亦著眼於個人資料在歐盟單一市場內之自由流動，以及歐盟整體數位經濟之發展，兼以計畫更進一步推動與促進歐盟境內「非屬個人資料」之流通、分析與發展之相關措施，企圖心可見一般。

GDPR 繁複之法律遵循義務造成業者不小之負擔與壓力，在推行之初，法規解釋之不明確確實對於企業經營造成風險，目前全世界仍在觀察中，而在 GDPR 之條文中存有若干可能對於數位經濟發展有利之措施，或許並沒有想像中便利與廣泛全面，但仍某程度展現 GDPR 之規範方向，數位經濟業者可考量並利用。歐盟以上作法未必係個人資料保護與數位經濟發展最佳之調適方式，但仍值得參考借鏡，讓我們拭目以待。👉

（以上為作者個人意見，未必代表理律法律事務所之立場或主張）

GDPR與我國個人資料保護法之比較分析

國發會法制協調中心參事 李世德

壹、前言

貳、GDPR 立法目的

參、GDPR 適用事項範圍

肆、GDPR 三大法域適用範圍

伍、GDPR 適用之客體、行為、相關主體

陸、GDPR 個資保護基本原則

柒、GDPR 控管者（蒐集主體）及處理者（受託者）義務

捌、GDPR 個人資料主體權利

玖、GDPR 個人資料之跨境傳輸規範

拾、GDPR 有關請求損害賠償救濟與行政裁罰規範

拾壹、小結

壹、前言

GDPR 是「General Data Protection Regulation」的簡稱，於我國國家發展委員會官方網站之中文翻譯為「一般個人資料保護規則」，其英文全稱為「Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC」，中文翻譯為「第 2016/679 號關於自然人資料處理及此類資料自由流通的個人保護規則，並取代 Directive 95/46/EC」，2018 年 5 月 25 日生效，共有 11 章，99 條。而「Regulation」（規

則)是歐洲聯盟(European Union, 簡稱歐盟)於歐盟基礎條約以外之三
次級法令中,具有能直接普遍適用於28個歐盟會員國¹,對會員國政府與
人民有全面拘束力之法律效果²。另外根據歐洲經濟區(European Economic
Area, EEA)協定第7條(a)款規定,非歐盟會員國之冰島,列支敦士登和
挪威,亦應適用GDPR。

我國《個人資料保護法》,簡稱《個資法》,取代電腦處理個人資料保護
法,修正條文分別於2012年10月1日及2016年3月15日生效,共6章,
56條,僅適用於我國,係內國法律,惟我國《個資法》與GDPR皆師承經濟
合作既發展組織(OECD)個人資料保護八大原則,且我國《個資法》研修
過程,不少條文意旨³參考GDPR前身之Directive 95/46/EC⁴相關規定,故
GDPR與我國《個資法》比較分析時,將可發現二者具有相似之處⁵。

比較分析必須有明確的比較主題或對象,尋找明確比較基礎,是比較分析
之首要工作。105年法務部委請范姜真熾教授、劉定基副教授、李寧修副教授
撰寫之「歐盟及日本個人資料保護立法最新發展之分析報告」第四章「歐盟、

¹ 法國、德國、義大利、荷蘭、比利時、盧森堡、英國、愛爾蘭、丹麥、希臘、葡萄牙、西班牙、芬蘭、瑞典、奧地利、波蘭、捷克、匈牙利、斯洛伐克、斯洛維尼亞、愛沙尼亞、拉脫維亞、立陶宛、馬爾他、賽普勒斯、羅馬尼亞、保加利亞、克羅埃西亞,計28國。

² 規則(regulation)、指令(directive)、決定(decision)等三者具有法律拘束力,另有建議(recommendation)與意見(opinion)二者則不具拘束力。「規則」係針對未來事務所為之一般抽象規定,能直接普遍適用於會員國,對會員國政府與人民有全面拘束力。「指令」與規則不同,通常以會員國為發布對象,只作原則性指示,要求會員國達成一定結果,容許會員國自己選擇執行之形式與方法。故指令不能直接適用但並不等於不具直接的法律效力。指令一般都規定有完成的期限,逾期不達成所要求之結果,須受司法審查之追究。「決定」是具體實施法規的行政措施,頒發對象可能是會員國或個人(自然人或法人),只具有特定的適用性,但對受文者有全面的法律拘束力。《歐洲聯盟法研究》,王玉葉著,元照出版社,2015年5月初版,第9頁。

³ 我國《個資法》第2條第1款、第6條第1項、第7條、第8條、第9條、第51條第1項第1款規定。

⁴ 歐洲議會及歐盟理事會於1995年10月24日公布(並於三年後之1998年10月24日生效)之歐盟指令第95/46/EC號,英文全稱為「Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data」,中文翻譯為「第95/46/EC號關於個人資料處理及此類資料自由流通的個人保護指令」;英文簡稱為「Data Protection Direction」,中文翻譯為「個人資料保護指令」。

⁵ 我國《個資法》第2條第1款、第6條第1項、第7條、第8條、第9條、第51條第1項第1款規定。

日本及我國個資法制之比較、分析」，即以獨立議題式之排列方式，例如：個人資料之定義與保護範圍、合法蒐集、處理及利用個資之要件、個資當事人之權利、跨國傳遞個資之規範、個資之安全維護及個資法施行之監督機制等議題，同時平行比較法制上差異。惟本次期刊主題是「歐盟 GDPR」，故本篇文章比較基礎，改以 GDPR 體系重要架構為主⁶，再輔以我國《個資法》類似規定，進行比較。另 GDPR 第 7 章「合作及一致性」、第 10 章「授權法及施行法」、第 11 章「最終條款」，屬歐盟會員國之間合作機制與施行安排規定，本具有特殊性，與我國《個資法》內國法性質，無共同比較基礎，不列入比較範圍。又 GDPR 第 6 章「獨立監管機關」及第 9 章「特殊處理情況之規範」，我國《個資法》亦無此專章項目，亦暫不列入比較。

貳、GDPR立法目的（GDPR第1條第1項規定）

制定 GDPR 係為規範關於保護個人資料處理與資料自由流通之兩大目的。個人資料之處理雖應有益於人類，但個人資料保護之權利，並非具有絕對性；故必須同時考量到其在社會上之作用，於符合比例原則下，兼顧其他基本權。⁷

【我國個資法】

我國《個資法》係為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用（《個資法》第 1 條規定）。故與 GDPR 立法目的相仿，應考量各種權利之平衡，而非僅為保護個人資料。

⁶ 本篇文章引用之 GDPR 條文中文翻譯內容，請參考國家發展委員會網站：首頁 / 主要業務 / 法制協調 / 個人資料保護專案辦公室 / 歐盟一般資料保護規則專區 / 歐盟 GDPR 法規 https://www.ndc.gov.tw/Content_List.aspx?n=F98A8C27A0F54C30

⁷ GDPR Recital 4.

叁、GDPR適用事項範圍（GDPR第2條規定）

一、適用事項範圍

該個人資料處理之技術方式，不論是：1. 全部或一部以自動化方式處理之個人資料；或者 2. 以非自動化方式處理個人資料，且形成或預計形成檔案系統（filing system）⁸之一部分者，才有 GDPR 適用。

二、不適用事項範圍

- （一）非屬歐盟法律規範範圍之活動過程。
- （二）歐盟成員國在執行屬於歐盟條約（TEU）有關共同外交和安全政策的具體規定範圍內之活動時。
- （三）自然人純粹的個人或者家庭活動。
- （四）主管機關為預防、調查、偵查、起訴刑事犯罪或執行刑事處罰的目的（包括防範和預防公共安全威脅）。因為上開處理行為另適用歐盟「主管機關為達預防、調查、偵查及追訴刑事犯罪或執行刑罰之目的，對於個人資料處理之保護及自由流通」第 2016/680 號指令。

【我國個資法】

GDPR 所稱廣義之「處理」行為，即包含我國個資法所稱「蒐集、處理、利用」行為（詳「伍」「我國個資法」二），故我國《個資法》所稱「蒐

⁸ 「檔案系統」係指依據特定標準可接近使用之個人資料所建構之任何檔案，不問是集中式、分散式或依功能性或地域性分散式之檔案（GDPR 第 4 條第 6 款規定）。

集」即以任何方式取得個人資料後，續進行狹義之「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，進而「利用」係指將蒐集之個人資料為處理以外之使用。故我國《個資法》適用之蒐集處理利用個人資料，亦須具有為建立或利用個人資料檔案⁹為前提，為適用事項範圍。

另有下列情形之一者，不適用我國《個資法》規定：

- (一) 自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。
- (二) 於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料（以上詳我國《個資法》第 51 條第 1 項第 1 款及第 2 款規定）。

此相當 GDPR 所稱「自然人純粹的個人或者家庭活動」之不適用事項範圍。

肆、GDPR三大法域適用範圍（GDPR第3條規定）

一、在歐盟範圍內設立業務據點的控管者或處理者

GDPR 適用於在歐盟範圍內設立業務據點的控管者或處理者（一般為某一組織，定義詳「伍、三」之說明）對個人資料的處理活動，無論其處理行為是否發生在歐盟範圍。

⁹ 指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合（我國個資法第 2 條第 2 款規定）。

二、沒有在歐盟範圍內設立業務據點的控管者或處理者

GDPR 適用於沒有在歐盟範圍內設立業務據點的控管者或處理者，對歐盟境內個人資料當事人的個人資料處理活動，其處理活動涉及：a. 向歐盟境內的個人資料當事人提供商品或服務（不論是否需要付款）；b. 監測發生在歐盟範圍內的個人資料當事人的行為。

三、國際公約

非在歐盟範圍內設立，但依控管者所在地根據國際公約法需適用歐盟成員國法律，則該控管者對個人資料的處理活動適用 GDPR。

【我國個資法】

公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法（我國《個資法》第 51 條第 2 項規定）。按我國《個資法》依屬地原則，不論我國人或外國人在我國領域內有違反我國《個資法》之行為，原則上應適用我國法規定¹⁰；至於在我國領域外蒐集、處理或利用個人資料行為，須合於下列要件，始有《個資法》之適用¹¹：

- (一) 從事蒐集、處理或利用行為者為我國之公務機關及非公務機關；
- (二) 所蒐集、處理或利用者為我國人民之個人資料。

故未在我國領域內設立業務據點的控管者或處理者，對我國領域內個人資料當事人的個人資料處理活動，我國《個資法》並無規範。

¹⁰ 法務部 102 年 6 月 6 日法律字第 10100088140 號函意旨參照。

¹¹ 法務部 107 年 3 月 12 日法律字第 10703502240 號函意旨參照。

伍、GDPR適用之客體、行為、相關主體

一、GDPR適用之客體——個人資料

(一) 屬 GDPR 適用之個人資料

1. 「個人資料」(personal data) 係指有關識別或可得識別自然人(「資料主體」, 即個人資料當事人, 下同) 之任何資訊; 可得識別自然人係指得以直接或間接地識別該自然人, 特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素(GDPR 第 4 條第 1 款規定)。
2. 「假名化」(pseudonymisation) 係指處理個人資料之方式, 使該個人資料在不使用額外資訊時, 不再能夠識別出特定之資料主體, 且該額外資料已被分開存放, 並以技術及組織措施確保該個人資料無法或無可識別出當事人(GDPR 第 4 條第 5 款規定)。

(二) 非屬 GDPR 所稱之個人資料

1. 匿名資料: 個人資料保護的原則不應適用於匿名資料, 即資料本身即非設及已識別的或可識別自然人的資訊, 或者將個人資料運用不可識別方式而成為不具有可識別性之資料, 不再適用 GDPR。¹²
2. GDPR 不適用於死者的個人資料。但會員國可提供有關處理死者個人資料的規則。¹³
3. 不適用於法人。¹⁴

¹² GDPR Recital 26.

¹³ GDPR Recital 27.

¹⁴ GDPR Recital 14.

二、GDPR適用之行為——處理

- (一)「處理」(processing)係指對個人資料或個人資料檔案執行任何操作或系列操作，不問是否透過自動化方式，例如收集、記錄、組織、結構化、儲存、改編或變更、檢索、查閱、使用、傳輸揭露、傳播或以其他方式使之得以調整或組合、限制、刪除或銷毀(GDPR第4條第2款規定)。
- (二)「側寫、剖析」(profiling)係指對個人資料任何形式之自動化處理，包括使用個人資料來評估與該當事人有關之個人特徵，特別是用來分析或預測有關當事人之工作表現、經濟狀況、健康、個人偏好、興趣、可信度、行為、地點或動向等特徵(GDPR第4條第4款規定)。

三、GDPR適用之相關主體

- (一)「控管者」(controller)係指單獨或與他人共同決定個人資料處理之目的與方法之自然人或法人、公務機關、局處或其他機構；依照歐盟法或會員國法決定處理之目的及方法，由歐盟法或會員國法律規定控管者或其認定之具體標準(GDPR第4條第7款規定)。
- (二)「處理者」(processor)係指代控管者處理個人資料之自然人或法人、公務機關、局處或其他機構(GDPR第4條第8款規定)。

【我國個資法】

一、我國個資法適用之客體——個人資料

(一) 屬我國《個資法》適用之個人資料

1. 「個人資料」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（我國《個資法》第 2 條第 1 款）。故與 GDPR 所稱指有關識別或可得識別自然人（「資料主體」）之任何資訊，意旨完全一致，至於例示內容（識別之參考資訊）或許不一致，但因不影響二者對個人資料解釋方向之相容性。
2. 我國《個資法》雖未規定「假名化」，但概念上仍得透過解釋我國《個資法》第 2 條第 4 款規定「編輯」之處理行為，包含「假名化」，如運用各種技術予以去識別化，而依其呈現方式，仍保有額外資訊得間接識別該特定個人者¹⁵，縱使該額外資料已被分開存放，仍與 GDPR 所稱之「假名化」法律效果相仿。

(二) 非屬我國《個資法》所稱之個人資料

1. 匿名資料：我國《個資法》雖未規定「匿名資料」，但概念上仍得透過解釋我國《個資法》第 2 條第 1 款規定「個人資料」之反面解釋，如公務機關或非公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個

¹⁵ 法務部 105 年 8 月 4 日法律字第 10503510730 號函意旨略以：資料經過提供者將直接識別個人資料加工處理成為間接識別個人資料，提供給學術研究機構進行彙整統計分析，嗣該機構再以無從識別特定當事人之方式為研究成果之發表，即為適法之特定目的外利用。

人資料，自無《個資法》之適用（法務部 103 年 11 月 17 日法律字第 10303513040 號函參照）。

2. 我國《個資法》所稱個人，指現生存之自然人（我國個資法施行細則第 2 條規定），不適用於死者的個人資料、法人資料，與 GDPR 一致。

二、我國個資法適用之行為——蒐集、處理、利用

（一）「蒐集」指以任何方式取得個人資料（我國《個資法》第 2 條第 3 款規定）。

（二）「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（我國《個資法》第 2 條第 4 款規定）。

（三）「利用」指將蒐集之個人資料為處理以外之使用（我國《個資法》第 2 條第 5 款規定）。

我國《個資法》前身，即電腦處理個人資料保護法，參考德國聯邦個人資料保護法細化個人資料行為之思考，將所規範之行為，細分為「蒐集、電腦處理、利用」，我國《個資法》亦延續此一區分方式「蒐集、處理（狹義）、利用」。GDPR 廣義之「處理」行為，即包含我國《個資法》所稱「蒐集、處理、利用」行為。至於「側寫、剖析」（profiling）行為，當然包含在我國《個資法》所稱「蒐集、處理、利用」行為中，惟尚無如同 GDPR 第 22 條規定，針對「側寫、剖析」行為另設特別規範。

三、我國個資法適用之相關主體

(一) 公務機關、非公務機關（我國通稱為蒐集主體）

1. 「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（我國《個資法》第 2 條第 7 款規定）。
2. 「非公務機關」指前款以外之自然人、法人或其他團體（我國《個資法》第 2 條第 8 款規定）。

我國《個資法》除自然人而蒐集、處理或利用個人資料與其職業或業務職掌無關者，不適用我國《個資法》外（我國《個資法》第 51 條第 1 項第 1 款規定修法理由參照），其餘「公務機關」及「非公務機關」蒐集、處理或利用個人資料行為，應有我國《個資法》適用，此與 GDPR 「控管者」（controller）概念相當。

(二) 受委託蒐集、處理、利用者

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，於我國《個資法》適用範圍內，視同委託機關（我國《個資法》第 4 條規定）。此與 GDPR 「處理者」（processor）概念相當。

陸、GDPR 個資保護基本原則（GDPR 第 5 條規定）

一、合法性、公正性及透明度（Lawfulness, fairness and transparency）

資料主體為合法、公正及透明之處理。

二、目的限制（Purpose limitation）

蒐集目的須特定、明確及合法，且不得為該等目的以外之後續處理；依照 GDPR 第 89 條第 1 項規定，為達成公共利益之目的、科學或歷史研究目的或統計目的所為之進階處理，不應視為不符合原始目的。

三、資料最少蒐集原則（Data minimisation）

適當、相關且限於處理目的所必要者。

四、正確性（Accuracy）

正確且必要時應隨時更新；考慮個人資料處理之目的，應採取一切合理措施，確保不正確之個人資料立即被刪除或更正。

五、完整性和保密性（Integrity and confidentiality）

處理應以確保個人資料適當安全性之方式為之，包括使用適當之技術上或組織上之措施，以防止未經授權或非法處理，並防止意外遺失、破壞或損壞。

六、儲存限制（Storage limitation）

資料主體之識別資料保存於一定形式，不長於處理目的所必要之期間；個人資料處理係單獨為達成公共利益之目的、科學或歷史研究目的或統計目的，且符合 GDPR 第 89 條第 1 項規定，實施適當之技術上及組織上之措施以確保資料主體權利及自由之要求者，該個人資料得被儲存較長時間。

七、說明責任（Accountability）

控管者應遵守並就其符合上開六大原則規定負說明責任。

【我國個資法】

我國《個資法》雖僅於第 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。」而未將各種個人資料保護原則逐一列出，但我國《個資法》，皆將上開 GDPR 所列個人資料保護基本原則精神，具體規範於相關條文（例如：第 6 條、第 8 至 11 條、第 15 條、第 16 條、第 18 條、第 19 條、第 20 條、第 27 條）。

柒、GDPR控管者（蒐集主體）及處理者（受託者）義務

一、控管者的義務概述

（一）非特種個人資料處理的合法性依據（GDPR 第 6 條規定）

1. 同意：

資料主體已同意為一個或多個特定目的處理其個人資料。資料主體的同意必須是明確的，自由的，具體的，知情的和明確的。因此，如果一個人在不完全且易於理解的情況下，不知道處理目的而給予同意，那麼它將不是有效的同意。單純沉默、預設為同意之選項或不為表示，皆不構成有效的同意。資料主體有權隨時撤回其同意（GDPR

第 7 條規定)。直接向兒童提供資訊社會服務之情況，如兒童年滿 16 歲，兒童之個人資料處理應屬合法。如該兒童未滿 16 歲，僅限於其法定代理人授權或同意之範圍內，該等處理始為合法（GDPR 第 8 條規定）。

2. 契約或類似契約關係：

處理係為向身為契約當事人之資料主體履行契約所必須者，或在締約前，應資料主體之要求，所必須採取之步驟。

3. 法律義務：

處理係控管者為遵守法律義務所必須者。

4. 重要利益：

處理係為保護資料主體或他人重大利益所必須者。

5. 公共利益：

處理係為符合公共利益執行職務或委託控管者行使公權力所必須者。

6. 合法利益：

處理係控管者或第三者為追求正當利益之目的所必須者，但該個人資料保護之資料主體之利益或基本權與自由優先於該等利益，特別是該資料主體為兒童時，不適用之。

(二) 特種個人資料處理的合法性依據（GDPR 第 9 條規定¹⁶）

揭露種族或人種、政治意見、宗教或哲學信仰或工會會員之個人資料、以及基因資料、用以識別自然人之生物特徵識別資料、與健康相關或與

¹⁶ 本條條文摘述，係參考 105 年法務部委請范姜真嫻教授、劉定基副教授、李寧修副教授撰寫之「歐盟及日本個人資料保護立法最新發展之分析報告」第 21 至 22 頁。

自然人之性生活或性傾向有關個人資料之處理，應予禁止。除非符合下列要件之一，始得為之：

1. 當事人表示明確之同意，但若歐盟法或各會員國之法令明訂特種資料處理之禁止不得藉由當事人同意而解除時，則不在此限。
2. 該處理為資料管理者或當事人主張其基於勞動法或社會安全或保護之法令所享有之權利所必要。
3. 該處理係為保護當事人或其他自然人具生存重要性之法益所必要，且當事人出於身體或法律上原因無法表示同意。
4. 該處理透過基於政治、世界觀、宗教或工會所設立之基金會、社團或其他組織提供適當保障，非以營利為目的且係於其法定權限範圍內所為，但該處理僅限於其成員或昔日成員或與為達成其業務目的而有經常性聯繫之人，且該個人資料在未經當事人同意前不得對外公開。
5. 欲處理之個人資料已明顯由當事人公開。
6. 該處理係為執行、行使或保護法律上之請求權或為法庭審理範圍內之司法職權所必要。
7. 該處理係依據歐盟法或會員國法令，與其所欲達成目的間具合理關聯性，維護個人資料保護權利之本質，並訂有保護當事人基本權利及利益之適當特殊措施，而基於有重大之公益理由，認有必要者。
8. 該處理係出於健康照護或為判斷受僱者工作能力之勞動醫學，為了醫學上之診斷、健康或社會領域之照護或治療或為了健康或社會領域之體系或服務之管理，依據歐盟法、會員國之法令或與擔任健康相關職業之成員間簽訂之契約，並符合 GDPR 第 9 條第 3 項所定要件及保障，而認有必要者。

表 1 其他要求落實 GDPR 之附隨義務

要求落實 GDPR 之附隨義務	內容
1.控管者根本義務	適當資料保護政策之實施。(GDPR第24條)
2.個資保護始於設計及預設	考量風險，不問係在決定處理方式時或係在處理中，或在預設情況下，控管者均應實施適當之科技化且有組織的措施，旨在實現資料保護原則。(GDPR第25條)
3.聯合控管者、設置代理人、選擇處理者之義務	(1) 兩個或兩個以上控管者共同決定處理之目的及方式時，應透明安排其各自履行GDPR所定義務之責任。(GDPR第26條) (2) 對歐盟內個人提供商品服務或進行監控，原則應設置代理人。(GDPR第27條) (3) 處理者之轉委託保留、契約義務、合規性確保。(GDPR第28條)
4.全面記載處理活動之義務	任一控管者及處理者應維護其負責之處理活動紀錄。(GDPR第30條)
5.處理過程安全性之義務	控管者需要實施適當的技術和組織措施，以確保與風險相稱的個人資料處理的安全層級。(GDPR第32條)
6.個資洩漏之通知義務	通知個資保護監管機關。(GDPR第33條) 通知個資當事人。(GDPR第34條)
7.個資衝擊影響評估	於特別使用新科技之處理方式，應於處理前，實行該處理對於個人資料保護之影響評估。(GDPR第35條)
8.事先諮商義務	當資料保護影響評估顯現高風險時，控管者應於處理前諮詢監管機關。(GDPR第36條)
9.設置個資保護長	公務機關、控管者或處理者大規模監控個人或處理特種個資、前科犯罪個資。(GDPR第37-39條)

9. 該處理係於公共衛生領域基於公益理由，例如為防範跨境之嚴重健康危害或為維護健康照護及醫藥產品的高品質及安全標準，並已依歐盟法或會員國法令採行維護當事人權利及自由之適當特殊措施，而認有必要者。
10. 該處理係依據歐盟法或會員國法令，與其所欲達成目的間具合理關聯性，維護個人資料保護權利之本質，並訂有保護當事人基本權利及利益之適當特殊措施，而依據 GDPR 第 89 條第 1 項基於公益之檔案儲存目的、學術或歷史研究目的以及統計目的，認有必要者。

(三) 前科及犯罪之個人資料處理的合法性依據

依 GDPR 第 6 條第 1 項規定處理涉及前科及犯罪之個人資料或相關安全措施，僅有下列情形之一者，始得為之：於公務機關控制下所為之處理，或歐盟或會員國法已為資料主體之權利與自由規範適當保護措施而授權之處理。任何全面性的前科紀錄僅限由公務機關控管保存（GDPR 第 10 條規定）。

(四) 其他要求落實遵守 GDPR 之附隨義務（參閱表 1）

二、處理者的義務

GDPR 顯著擴展了控管者和處理者的義務，最值得注意的是，過去 Directive 95/46/EC95 指令時代，處理者並不用直接負責歐盟個人資料保護法規之遵循責任，現在 GDPR 對處理者亦比照控管者，直接增設相關遵循法律之義務，例如：處理過程安全性之義務、個資洩漏之通知義務、全面記載處理活動之義務、設置個資保護長及設置代理人。

三、鼓勵控管者及處理者參與行為守則及驗證機制

遵守 GDPR 第 40 條所定經批准之行為守則或第 42 條所定經核准之驗證機制，得作為控管者及處理者遵守其義務之證明。

【我國個資法】

一、我國個資法蒐集主體義務

相較 GDPR 對控管者義務規範之多元化及細節化，我國《個資法》相形之下，較為單純：

(一)「公務機關」義務規定

1. 非特種個人資料蒐集、處理利用的合法性依據，於我國《個資法》第 15 條、第 16 條規定。
2. 特種個人資料蒐集、處理利用的合法性依據，於我國《個資法》第 6 條規定，亦同 GDPR 採原則禁止例外允許之立法模式。
3. 個人資料檔案安全維護義務，於我國《個資法》第 18 條規定。
4. 個人資料外洩通知當事人義務，於我國《個資法》第 12 條規定。
5. 公告保有之個人資料檔案型態資訊，於我國《個資法》第 17 條規定。

(二)「非公務機關」義務規定

1. 非特種個人資料蒐集、處理利用的合法性依據，於我國《個資法》第 19 條、第 20 條規定。
2. 特種個人資料蒐集、處理利用的合法性依據，於我國《個資法》第 6 條規定，與公務機關一同規範。
3. 個人資料檔案安全維護義務，於我國《個資法》第 27 條規定。
4. 個人資料外洩通知當事人義務，於我國《個資法》第 12 條規定。

表 2 GDPR 個人資料主體權利

個人資料當事人權利	內 容
1.受告知權（GDPR第13條、第14條）	從資料主體或他處蒐集其有關其之個人資料時，控管者應於取得個人資料時，提供資料主體有關應告知之資訊。
2.查閱權（GDPR第15條）	資料主體有權向控管者確認其個人資料是否正被處理，於此情形者，資料主體應有權接近使用其個人資料相關資訊。
3.更正權（GDPR第16條）	資料主體應有權使控管者更正其不正確之個人資料。
4.刪除權（GDPR第17條）	一定情形下（例如：個人資料對於蒐集或處理目的不再需要者）資料主體應有權使控管者刪除其個人資料。
5.制限處理權（GDPR第18條）	一定情形下（例如：資料主體質疑其個人資料之正確性，而給予控管者驗證該個人資料正確性之期間）資料主體應有權限制控管者之處理。
6.資料可攜權（GDPR第20條）	資料主體應有權以有結構的、通常使用的、機器可讀的形式，接收其提供予控管者之資料，並有權將之傳輸給其他控管者。
7.異議權（GDPR第21條）	資料主體拒絕依GDPR第6條第1項第e點或第f點規定所為有關其個人資料之處理。除非控管者證明其處理有優先於資料主體權利。另有行銷拒絕權利、為科學或歷史研究目的或統計目的所為者之拒絕權。
8.自動化數位剖析許可權（GDPR第22條）	資料主體應有權不受僅基於自動化處理（包括數位剖析）所做成而對其產生法律效果或類似之重大影響之決策所拘束。

二、我國《個資法》並未對受委託蒐集處理利用者，課予相關義務。

三、我國《個資法》雖無規定鼓勵蒐集主體踐行相關行業制定行為守則或通過驗證機制，但不影響蒐集主體尋求相關自律規範之實踐。

捌、GDPR個人資料主體權利

參見表 2（頁 87），可知 GDPR 中個人資料當事人權利內容。

【我國個資法】

個人資料當事人（資料主體）就其個人資料依我國《個資法》規定行使之下列權利，不得預先拋棄或以特約限制之：

- （一）查詢或請求閱覽。
- （二）請求製給複製本。
- （三）請求補充或更正。
- （四）請求停止蒐集、處理或利用。
- （五）請求刪除（我國《個資法》第 3 條規定）。

此為五大個人資料當事人基本權利，其詳細規範於我國《個資法》第 10 條至 14 條規定。其次，個人資料當事人受告知之權利，係規範於我國《個資法》第 8 條及第 9 條規定。再者，有關於個人資料當事人對合法行銷行為及一般可得來源資料蒐集之異議權，分別規範於我國《個資法》第 20 條第 2、3 項及第 19 條第 2 項規定。除此之外，我國《個資法》明顯無「資料可攜權」

、「自動化數位剖析許可權」、「個人資料對於蒐集或處理目的不再需要者之刪除權（被遺忘權）」規範。

玖、GDPR個人資料之跨境傳輸規範（詳見本期「GDPR之國際傳輸」一文）

（一）適足性認定（GDPR 第 45 條規定）。

（二）未經適足性認定，應有適切安全管理措施（GDPR 第 46 條規定）。

1. 採用標準契約條款（SCC）、監督機關承認之契約條款、遵循行為守則、取得驗證。

2. 採用拘束的企業準則（BCR）（GDPR 第 47 條規定）

（三）無適切安全管理措施時之例外措施（GDPR 第 49 條規定），例如：明示的本人同意、本人於契約履行必要場合、公共利益、本人重大利益保護等。

【我國個資法】

我國《個資法》對公務機關部分未設國際傳輸個人資料之限制，僅有針對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（我國《個資法》第 21 條規定）。

故相較於 GDPR 多層次國際傳輸法規體系，我國《個資法》在中央目的事業主管機關未限制國際傳輸個人資料前，非公務機關基於合法蒐集、處理、利用要件，即可將個人資料作跨國（境）之處理或利用。

拾、GDPR有關請求損害賠償救濟與行政裁罰規範

一、民事責任

因違反 GDPR 而遭受物質上或非物質上之損害時，任何人應有權利自控管者或處理者就其損害獲得賠償。若控管者或處理者可證明其等對於造成損害之事件不可歸責時，始得免除賠償責任（GDPR 第 82 條規定）。資料主體應有權委任依會員國法合法設立、以公益為目的，且在個人資料保護領域活躍之非營利機構、組織或社團，以及於會員國法有規定時，代資料主體行使其 GDPR 第 82 條所定收受賠償金之權利（GDPR 第 80 條規定）。

二、行政裁罰（GDPR第83條規定）

第一、違反本規則有關控管者及處理者之附隨義務、驗證機構之義務或監管機構之義務者

違反下列 GDPR 規定者，最高處以 10,000,000 歐元之行政罰鍰，或如為企業者，最高達前一會計年度全球年營業額之百分之 2，並以較高者為準：(a) 第 8 條、第 11 條、第 25 條至第 39 條及第 42 條及第 43 條所定控管者及處理者之義務；(b) 第 42 條及第 43 條所定驗證機構之義務；(c) 第 41 條第 4 項所定監管機構之義務。

第二、違反有關資料處理之基本原則、個人資料國際傳輸之規定、侵害 GDPR 所定資料主體之權利、或違反依照 GDPR 通過之會員國法律所定之任何義務者

違反下列 GDPR 規定者，最高處以 20,000,000 歐元之行政罰鍰，或如為企業者，最高達前一會計年度全球年營業額之百分之 4，並以較高者為準：(a) 第 5 條、第 6 條、第 7 條及第 9 條所定處理之基本原則，包括同意之條件；(b) 第 12 至 22 條所定資料主體之權利；(c) 第 44 條至第 49 條所定個人資料移轉至第三國或國際組織之接收者；(d) 依照第 9 章通過之會員國法律所定之任何義務；(e) 違反監管機關依第 58 條第 2 項規定之命令或暫時性或終局性之處理限制或停止資料傳輸，或未提供進入而違反第 58 條第 1 項規定；

第三、違反監管機關依 GDPR 第 58 條第 2 項規定之命令者

最高處以 20,000,000 歐元之行政罰鍰，或如為企業者，最高達前一會計年度全球年營業額之百分之 4，並以較高者為準。

【我國個資法】

一、民事責任

(一) 公務機關：

公務機關違反我國《個資法》規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限（我國《個資法》第 28 條第 1 項規定）。對公務機關採幾近無過失責任，更嚴格於 GDPR。

(二) 非公務機關：

非公務機關違反我國《個資法》規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限（我國《個資法》第 29 條第 1 項規定），對非公務機關採舉證倒置責任，與 GDPR 相同。

(三) 公務機關及非公務機關定額賠償及總額上限賠償：

以每人每一事件新臺幣 500 元以上 2 萬元以下計算。對於同一原因事實造成多數當事人權利受侵害之事件，原則上合計最高總額以新臺幣 2 億元為限（我國《個資法》第 28 條第 3、4 項，第 29 條第 2 項規定）。此係我國《個資法》獨有特色，GDPR 所無。

(四) 團體訴訟：

對於同一原因事實造成多數當事人權利受侵害之事件，財團法人或公益社團法人經受有損害之當事人 20 人以上以書面授與訴訟實施權者，得以自己之名義，提起損害賠償訴訟（我國《個資法》第 32 條至第 40 條規定），此與 GDPR 之團體訴訟相仿。

二、行政裁罰（僅限對非公務機關）

(一) 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣 5 萬元以上 50 萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：一、違反第 6 條第 1 項規定。二、違反第 19 條規定。三、違反第 20 條第 1 項規定。四、違反中央目的事業主管機關依第 21 條規定限制國際傳輸之命令或處分（我國《個資法》第 47 條規定）。對非公務機關違背蒐集處理利用要件及限制國際傳輸命令，法律預設之行政處罰較重。

- (二) 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣 2 萬元以上 20 萬元以下罰鍰：一、違反第 8 條或第 9 條規定。二、違反第 10 條、第 11 條、第 12 條或第 13 條規定。三、違反第 20 條第 2 項或第 3 項規定。四、違反第 27 條第 1 項或未依第 2 項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法（我國《個資法》第 48 條規定）。
- (三) 非公務機關無正當理由拒絕進入、檢查或處分，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣 2 萬元以上 20 萬元以下罰鍰（我國《個資法》第 49 條規定）。

拾壹、小結

此次 GDPR 面臨數據全球化現象，擴大法域適用範圍和增設多層次之權利義務規定，讓我國《個資法》於進行解釋及修法活動，有豐沛之外國立法例足供參考。惟我國也面臨各種智慧型手機、APP 軟體、生物特徵辨識、雲端服務、大數據分析、物聯網、人工智慧技術（機器人、自動駕駛）等等科技應用成果，出現於各種政府服務或商業應用領域，甚至已形成所謂的數位經濟（Digital economy），伴隨產生個人資料保護與管理議題之解決方案需求，讓我國《個資法》的成長，更需借鏡 GDPR 法制之實踐經驗。故 GDPR 開始施行後，持續關注 GDPR 各種規範之實證性效果，未來將有助於我國《個資法》與 GDPR 之間，進行更深層之比較分析。🌐



特別企劃

SPECIAL REPORT

區塊鏈國際趨勢

國發會綜合規劃處

- 壹、區塊鏈的特點與發展
- 貳、主要國家／城市區塊鏈政策
- 參、未來推動方向
- 肆、結語

近年來，區塊鏈（Blockchain）已成為國際間一個熱門議題，許多國家已意識到區塊鏈技術本身與其他技術（如人工智慧、大數據、物聯網）的融合，帶來的龐大商機與潛在應用價值，紛紛從國家戰略層面，支持本國區塊鏈技術研究與應用發展，厚植國家競爭力。經濟合作暨發展組織（OECD）於今（2018）年9月4至5日在法國巴黎舉辦全球首次「OECD 區塊鏈政策論壇」國際研討會，吸引來自各地超過500位公、私部門高階決策者及學者專家，共同探討區塊鏈對全球經濟的潛在衝擊、對隱私與網路安全的意涵，及有效運用區塊鏈擴大包容性成長、促進綠色成長與永續性、強化政府治理及執行等，顯見區塊鏈在數位經濟時代下的重要性。

壹、區塊鏈的特點與發展

世界經濟論壇（WEF）指出，區塊鏈是顛覆性的「通用型科技」（General Purpose Technology, GPT），其作用如同過去工業革命的蒸汽機、電力與網際網路一樣，影響整體經濟結構變化、社會秩序與法規監管的制定，區塊鏈革命因此被稱為第四次工業革命；另 OECD「2017 數位經濟報告」指出，區塊鏈與人工智慧係影響未來全球經濟、社會與文化的最重要數位科技，將大幅改變現代商業模式與生活方式。

一、區塊鏈的起源與特性

區塊鏈是一種分散式帳本技術（Distributed Ledger Technology, DLT），使網際網路能夠實現「價值移轉」，因此又被稱為升級版的網際網路。

過去傳統經濟中，人們因缺乏對彼此的信任，在多數的情況下，必須透過中介機構，才能完成價值移轉行為；區塊鏈的起源就是要設計一套信任機制，不須透過中介機構，完成各種有價資產的交易，並且在確保價值傳送完成後，能夠精確改變交易雙方的資產數量，讓一方資產增加、另一方資產對應減少。

舉例而言，當某甲想要給某乙 100 元時，按照目前的方式，是透過銀行轉帳來完成，交易完成後，某甲的帳戶會減少 100 元、某乙的帳戶會增加 100 元；區塊鏈的設計原理是將這筆交易傳送到網路上參與交易的每一個人，由每位參與者共同確認，並記錄在每位參與者的帳本上，以確保交易資訊真實性與正確性。

相較於傳統以銀行為金融中介的交易模式，區塊鏈技術提供「去中心化」、「匿名性」、「不可竄改性」、「可追蹤性」及「加密安全性」等特色，可協助商業網絡中的各參與方提升互信及執行效率，實現價值在網際網路的流動，區塊鏈因而被稱為信任機器。

二、區塊鏈的應用發展

目前區塊鏈的應用領域可概分為「幣圈」與「鏈圈」兩類，前者以各類虛擬貨幣為主，後者強調在「區塊鏈 + 各行各業」的拓展。整體而言，區塊鏈技術與應用係朝「創新、融合、開放、共享」的生態體系發展。

區塊鏈最早的應用是在 2009 年的比特幣 (Bitcoin)，其後許多網路社群亦發行其虛擬通貨，如以太坊 (Ethereum) 發行的以太幣 (Ether)，及應用在國際金融交易為主的瑞波幣 (Ripple) 等。此外，由於金融系統的本質就是在處理有價資產在社會間的流動，因此在金融領域的應用上，舉凡交易結算、資金移轉、貿易融資、保險、證券等，都可以運用區塊鏈技術來增進效率。例如：今年 8 月世界銀行 (World Bank) 宣布將發行全球首檔區塊鏈債權「區塊鏈新債發行工具」(Blockchain Offered New Debt Instrument，簡稱 bond-i)，運用區塊鏈技術創造、分配、移轉、管理債券，結算時間由五天縮短為數秒，可大幅提升其營運效率。

近期，區塊鏈的應用領域已拓展至智慧城市、產業供應鏈、能源管理、數位娛樂及公共治理等非金融領域，甚至是跨國型的國際援助亦著手應用。例如：2017 年 5 月聯合國世界糧食計劃署 (World Food Program) 即運用以太

坊的區塊鏈技術，透過加密貨幣憑證換券，提供敘利亞難民換取糧食及物資，不但可節省援助難民計畫的執行成本、提高記帳速度，並能落實難民個資及隱私的保護。

貳、主要國家／城市區塊鏈政策

隨著區塊鏈技術益趨普及，各國政府對區塊鏈潛在應用價值及風險認知不斷提升，乃積極強化法規監管與創新科技雙向的包容互動，推動區塊鏈正向發展。其中又以愛沙尼亞、英國、阿拉伯聯合大公國與杜拜酋長國的戰略框架較具代表性，重點說明如次：

一、愛沙尼亞

愛沙尼亞是波羅的海三國中，面積最小、人口最少的國家，但卻是全球電子化政府整合性最高的國家，也是區塊鏈應用最早的國家，其透過結合電子化政府與發展數位科技的經濟發展策略，成功帶領國家由蘇聯計畫經濟體制下的農工生產結構轉型為數位國家。

回顧愛沙尼亞數位轉型歷史，其在 2001 年建立數據交換網路「X-road」系統，將各行政機關零散的資料庫連結在一起，是當前世界上最先進的國民資料庫，為數位運作打造不可或缺的重要基礎設施；2002 年發行晶片身分證，其國民只要透過晶片身分證，就能夠透過國民資料庫接受所有行政服務；2007 年為強化資訊安全防護，運用區塊鏈技術，在原有的電子簽章系統上，

開發加密簽章和無鑰簽章基礎設施（Keyless Signature Infrastructure, KSI），強化公共領域的資訊安全度。在這三項的基礎設施上，愛沙尼亞成為全球區塊鏈進展最快、應用範圍最廣的國家，並提供許多先進的公共服務，包括：電子內閣（e-Cabinet）、電子投票（i-Voting）、電子報稅（e-Tax）、電子警察（e-Police）、電子健康管理（e-Health）、電子教育（e-Education）、電子公司管理（e-Business）等。

2014 年愛沙尼亞推出全球首個跨國性「數位公民」（e-residency）策略，透過發行電子身分證，號召線上商務移民，為亟具國家戰略高度的代表性策略，不僅填補愛沙尼亞商務投資與勞動力的不足，更加速其與全球科技發展及產業創新的連結。擁有數位公民身分者，可以合法開立愛沙尼亞銀行帳戶、進行線上商務支付與轉帳、簽署具法律效力的數位文件，及申報與繳交稅賦等，亦可在歐盟進行商務貿易，同享歐盟成員的相關優惠。

2017 年 6 月，愛沙尼亞進一步宣布與盧森堡簽署協議，設立全球首座「數位大使館」（e-Embassy）。透過在海外設立具正式大使館地位的海外資料中心，備份國家財政、社會保險、地籍資料等重要資料，在國內數據資料發生突發事故時，數位大使館仍能提供資料，確保國家的正常運作，是愛沙尼亞國家發展與資料管理總體戰略的重要一環。

二、英國

英國作為全球金融重鎮，其政府十分重視區塊鏈技術的發展及對金融科技及政府治理的影響，並領先各國，率先發布首個全球區塊鏈政策白皮書。自 2015 年起，英國政府發布與施行之區塊鏈相關重要政策重點分述如下：

英國商業、創新與技能部（BIS）科學辦公室（Government Office for Science）2015 年 3 月發布「金融科技未來—英國作為世界金融科技領導者」（FinTech Futures: The UK as World Leader in Financial Technologies）白皮書，建議政府聚焦虛擬通貨及區塊鏈等新興技術，以促進金融服務轉型，提供客製化金融服務，並建議運用「監理沙盒」（regulatory sandbox）機制，打造一個兼顧金融科技創新與監管「安全空間」（safe space）。

科學辦公室 2016 年 1 月續發布「分散式帳簿：超越區塊鏈」（Distributed Ledger Technology: Beyond Blockchain）白皮書，為全球首個由國家層面，針對區塊鏈未來發展應用進行全面評估，並提出研究建議的報告（各章節重點摘要如表 1）。報告強調區塊鏈在公共服務應用的重要性，可減少詐欺、貪汙、人為錯誤及書面審查作業等，提高行政效率，並重塑政府與人民在資料共用、透明度及信任關係。

英國政府 2016 年 4 月正式啟動全球首個監理沙盒機制，提供區塊鏈新創企業安全創新環境；2018 年 7 月發布的第四輪監理沙盒測試申請結果，共有 69 家公司遞交申請書，29 家成功入選，其中已有超過 40% 的公司與分散式帳本技術相關，包括：發行自動債券或股權、提供保險服務等。

表 1 英國區塊鏈政策發展方向

發展方向	建議與說明
願景 (Vision)	<ul style="list-style-type: none"> 透過支持區塊鏈新興生態系統、早期試驗，及定位英國成為區塊鏈全球領導者等三個面向，提升英國政府的透明度與問責性 (accountability)
技術 (Technology)	<ul style="list-style-type: none"> 區塊鏈的許多應用仍在發展初期，還必須解決隱私權保護、效能及擴充性等問題。 但相關技術的進展相當快速，已經可以預見政府與企業因區塊鏈而運作的更有效率，也會有更多基於安全且共享資料而出現的新產品與新服務，引發數位貨幣及其他的全球性變革。
治理與法規 (Governance and Regulation)	<ul style="list-style-type: none"> 由於法律與技術 (軟硬體) 共同規範了數位經濟中的活動，在制定管制規範時，需將兩者同時併入考量，尋求最恰當的組合方式。 區塊鏈系統基本上沒有法人組織能為系統中的活動負責，因此政府應考慮藉由影響技術規範 (如設定公用標準及建立屬於政府的私有鏈或聯盟鏈) 來管制區塊鏈系統，而不是只依賴法律規範。 決策者亦應體認技術規範對金融體系的影響，並考慮如何將這樣的影響納入管制體系，以降低遵循成本。
安全與隱私性 (Security and Privacy)	<ul style="list-style-type: none"> 區塊鏈系統有多種型式 (私有鏈、聯盟鏈、公有鏈)，分別在安全與隱私方面，帶來不同的機會與威脅。在應用前必須先分析業務與安全上的需求，以決定採取哪種系統。 例如，聯盟鏈系統適用在銀行間進行支付、結算與清算，對安全和性能的要求較公有鏈系統高。
破壞性創新潛力 (Disruptive Potential)	<ul style="list-style-type: none"> 區塊鏈技術為現有商業與政府治理模式形成重大的挑戰，其引發的創新，不只將改變商業結構，最終亦將改變經濟與社會運作與管理的方式。這些潛在的變革應經過試驗階段，以發掘其在實際運作上、法律上及政策上的意涵。 對區塊鏈系統應有更多的研究，以瞭解應用區塊鏈技術的成本與效益，讓政府能避免不必要的社會衝突，並發現更多可以節省成本的空間及可利用的機會。

表 1 英國區塊鏈政策發展方向

發展方向	建議與說明
在政府中的應用 (Application in Government)	<ul style="list-style-type: none"> • 區塊鏈應用在政府公共服務，將有助於減少成本、增加透明度、提升普惠金融（financial inclusion），及促進創新與經濟成長。 • 以保護關鍵基礎設施、就業及退休金部門、強化國際救助系統、減少市場摩擦、歐洲增值稅等五個案例，說明應用區塊鏈的目的、預期成果及技術成熟度。
全球視野 (Global Perspective)	<ul style="list-style-type: none"> • 區塊鏈在建立全球合作夥伴信任關係、強化社群協作具有應用潛力，有助於處理像避稅、洗錢、非法貿易等全球性議題。

資料來源：英國「分散式帳簿：超越區塊鏈」白皮書（2016）。

三、阿拉伯聯合大公國與杜拜酋長國

阿拉伯聯合大公國副總統兼總理、杜拜酋長阿勒馬克圖姆（Al Maktoum）於2016年10月先提出「杜拜區塊鏈戰略」（Dubai Blockchain Strategy），並在2018年4月再宣布「阿聯區塊鏈戰略」（UAE Blockchain Strategy），將區塊鏈技術提升為更高層級的國家整體戰略。

杜拜掌握舉辦「2020杜拜世界博覽會」（Expo Dubai 2020）的機會，發布區塊鏈戰略，由「政府效率」、「產業創造」、「國際領導地位」三大支柱，在2020年前打造成為全球第一個公共服務與相關交易全部使用區塊鏈技術的政府，營造便捷經商環境，帶動企業發展，強化杜拜在中東的商業領導地位。

三大支柱	目標	說明
政府效率	100%應用在杜拜政府（2020年前）	<ul style="list-style-type: none">• 透過區塊鏈發展無紙化公文處理• 增加2,510萬小時的生產力• 減少1.14噸碳排放• 避免4.11億公里的公文旅行
產業創造	1,000個新公司成立（2020年前）	<ul style="list-style-type: none">• 可能受惠產業包括不動產、金融科技與銀行業務、健康照護、運輸、都市規劃、智慧能源、觀光等
國際領先地位	27國共同參與促進全球旅遊	<ul style="list-style-type: none">• 國際旅客可使用出發前檢驗通過的護照、簽證與安檢，享受快速通關• 可使用出發前檢驗通過的駕照與租賃契約，享受便捷移動

資料來源：Dubai Future Foundation、Smart Dubai 網站資料。

2017 年 2 月杜拜宣布啟動公共服務策略「Dubai 10X」，其中 10 代表要保有領先全球 10 年的地位，X 則代表要跳脫原有思考框架，2017 年共計推出 160 個區塊鏈應用專案，包括：車輛管理、旅遊服務、學術證書認證等；2018 年 2 月啟動第二期專案「Dubai 10X 2.0」，強化部門間的合作，加速顛覆性突破的實現，以公共服務質量與效率提升 10 倍作為最終目標。

今年 4 月，區塊鏈戰略提升至整個阿拉伯聯合大公國，目標是在 2021 年前將 50% 的政府交易都運用區塊鏈技術來完成。阿聯政府認為，區塊鏈技術有助於節省時間與資源，並可讓民眾在適合他們工作與生活的時間與地點下進行各種政府交易。透過區塊鏈技術的應用，將可節省近 30 億美金的交易成本，同時每年亦節省 3.98 億的紙本文件及 7,700 萬的工作時數。

叁、未來推動方向

目前國內區塊鏈技術正處於運用發展初期，政府部門已積極擴大區塊鏈在公共服務的可能性研究，並提前防範可能的各種潛在風險，例如：央行與金管會已著手分析數位貨幣對金融體系與總體經濟的影響。國發會對於區塊鏈發展亦相當重視，陳主任委員美伶於今年 7 月 2 日應邀出席亞洲區塊鏈聯盟（Asia Blockchain Alliance）舉辦的「2018 年亞洲區塊鏈高峰會」（2018 Asia Blockchain Summit）致詞時，提出政府未來推動區塊鏈發展的四大方向：

一、鼓勵區塊鏈新創產業發展，協助各產業導入區塊鏈技術，加速產業轉型升級

臺灣擁有優秀的資通訊技術人才及完整的資通訊產業供應鏈，具備發展區塊鏈產業的必備基礎條件，且政府對區塊鏈發展持開放態度，未來政府將加大政策上的支持力道，除透過充裕早期資金等措施持續優化新創事業投資環境，並加快開放資料（Open Data）工作，擴大巨量資料（Big Data）的產業應用，也將繼續鼓勵產業對區塊鏈的加值應用，針對實際問題提出創新解決方案，產生更具競爭力的服務和產品。

二、完善國內區塊鏈經濟監管法規的制定與詮釋，為區塊鏈產業發展提供必要的制度保障

為讓「企業廣泛受益、公眾普遍受惠」，政府必須維持創新與監管的動態平衡與風險控管。因此，政策重點將強調提供服務而非管制，期許能做到「法律沒有禁止的，原則上就是可以」，讓區塊鏈產業的自律精神與創業家精神都有更大的發揮空間。

三、檢視區塊鏈技術及服務與國際間個資保護相關要求的接軌

由於歐盟「一般資料保護規則」（GDPR）部分規定與區塊鏈架構有所衝突，例如：區塊鏈的「不可篡改性」特性與GDPR的「被遺忘權」可能有所抵觸，目前國發會已成立個人資料保護專案辦公室，後續將就相關議題進行研議規劃。

四、儘速將區塊鏈技術導入公共治理解決方案

國發會今年 5 月下旬曾率團拜訪德國非營利基金會 IOTA，瞭解 IOTA 所開發之另一種分散式帳本技術－ Tangle －的使用案例，以及在數位治理的應用開發。未來國發會將透過舉辦臺美與臺歐盟數位經濟論壇，持續引入美國與歐盟最新與最佳的推動經驗與措施，做為臺灣推動數位公共治理的借鏡。

肆、結語

在數位科技主導全球經貿實力消長的新時代，政府已將建設數位經濟列為施政重點。面對區塊鏈技術的快速發展，臺灣必須要善用此一技術，在各領域中找到獨特的優勢，實現「區塊鏈+」的發展潛力，同時政府也將採取行動，完善法規環境機制，鼓勵產業的升級與創新，引領臺灣朝向數位國家發展與轉型。🌀

臺中市畢業證書區塊鏈應用案例

臺中市政府資訊長 蕭景燈

臺中市西區大同國小教師 蕭聖哲

壹、結合內外部資源共同推動

貳、技術架構與流程設計

參、實作成果

肆、閱讀認證寫入區塊鏈，讓數位公民管理自己的數位資產

伍、為數位原生代打造新世代的應用

區塊鏈技術的第一個應用是數位貨幣，因此最初對此技術的探討多圍繞在金融財務相關領域，其不可竄改的基本特性讓區塊鏈不只是數位貨幣，也可以運用在任何價值的轉移交易、資料紀錄保存與跨機構共享，如再搭配智能合約，授權程式於滿足特定條件時不需人力介入自動執行，如此也增加了透明度與效能，對創業家而言區塊鏈意味著商業機會，但對提供公共服務的公部門而言，此項技術開啟了政府對人民服務的新模式。

對這個尚在探索階段的技術，各國政府投入的資源各異，努力的方向也不同，去（2017）年9月 Deloitte 發表了一份名為「區塊鏈將轉變公部門？」（Will blockchain transform the public sector?）¹ 的報告，報告中整理了包含

¹ <https://www2.deloitte.com/insights/us/en/industry/public-sector/understanding-basics-of-blockchain-in-government.html>

數位貨幣等 10 個公部門最積極推動的區塊鏈應用項目。此份報告在最終提出了建議，認為眾多方向中「身分管理」、「土地所有權登記」與「投票」是政府部門最能夠發揮區塊鏈價值的三項應用。

壹、結合內外部資源共同推動

臺中市政府在 2017 年起即思考區塊鏈運用於市民服務的可行性，經過內部討論，認為身分管理結合數位資產是適合在市府層級推動的應用，於同年 10 月與國家實驗研究院國家高速網路與計算中心簽訂合作備忘錄（圖 1），選定「畢業證書區塊鏈 PoC」為三個合作項目之一。畢業證書可以視為畢業生的無形資產，透過將此無形資產數位化，記錄在區塊鏈上，讓此項資產與畢業生的身分連結起來，將來對於此項資產的查詢或交易，任意第三方都不須透過原發證學校就可以進行畢業證書的驗證，這樣的過程沒有中介者，簡化了作業負擔，也提升了效益。

在市府內，這個 PoC 由資訊中心與教育局共同推動，並與教育局資訊教育暨網路中心相互配合，教網中心過去幾年負責 OpenID 單一帳號認證業務，亦是屬於身分管理的一環，兩個機制各司其職，透過介面設計達到互通，讓服務的整體性更佳。而教網中心原本就與學校行政人員與學生互動密切，因此可以負擔起在第一線服務使用者的角色。

貳、技術架構與流程設計

為了讓使用有個友善的操作介面，我們採用三層網路架構，包含後端底層的鏈，提供查詢的 Web Server，以及使用者端的瀏覽網頁呈現，圖 2 即是



圖 1 臺中市政府與國家實驗研究院國家高速網路與計算中心合作備忘錄

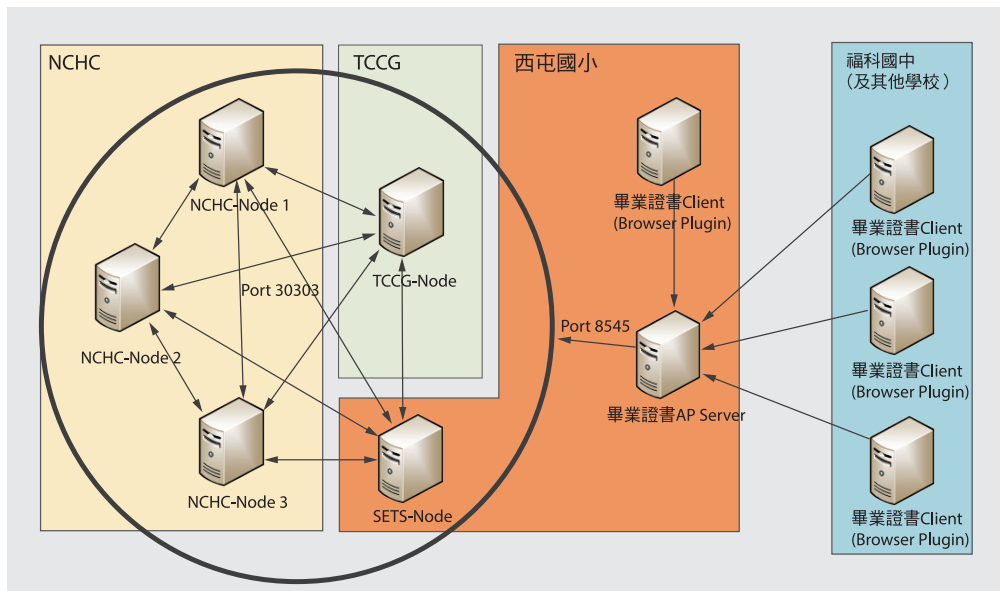


圖 2 三層網路架構示意

此三層網路架構之示意。

此外，我們選擇了以太坊 Ethereum 做為區塊鏈底層平台，採用聯盟鏈架構，在圖 2 中顯示的聯盟鏈由五個節點組成，其中三個節點分別位於國網中心（NCHC）新竹、臺中、臺南三處機房，臺中市政府（TCCG）內另有一個節點，上述四個節點承擔運算工作，最後一個節點則置於臺中教網中心的西屯國小（SETS）機房，這個節點也擁有鏈上完整的資料，但不負責運算而是與網站伺服器配合提供使用者查詢與瀏覽等服務。

本系統目前提供兩個主要機制，一是發行數位畢業證書至區塊鏈，二是自區塊鏈取出資料已驗證的數位畢業證書內容與簽署資訊；另有設計撤銷數位畢業證書機制會在日後版本新增。

數位畢業證書的發行由畢業生或是校方發起均可，最核心的步驟是校方對數位檔案中畢業證書記載內容進行審查，審查通過後，校方人員以審查人員的

私鑰則對此數位版本簽署，這相當於在實體複本蓋上「與正本相符」的戳記，並將此簽署過的文件加密儲存至分散式檔案系統 InterPlanetary File System (IPFS) 並寫入區塊鏈。此簽署文件以 JSON Web Signature 格式提供給畢業生留存，我們也設計了較易攜帶與流通的 QR Code 圖片格式讓畢業證書所有人持有。

當畢業生繼續升學，進入下一階段的學校，新學校需驗證該名新生是否已由前一所學校畢業，過往普遍的方式就是要求新生繳交畢業證書，學校人員以肉眼查核；此系統提供了一個新的途徑，畢業生只需提交上述的 QR Code 圖片（當場出示或是透過電子郵件寄送），收到這個 QR Code 的一方可以用行動裝置掃描，連上驗證伺服器啟動本系統的驗證流程，當資料驗證無誤後，系統會回覆對應此 QR Code 的數位畢業證書下載點，此時驗證方由 IPFS 取回數位畢業證書就算是完成了 Proof of Existence，也就是相信有一筆畢業證書曾經發行並在此區塊鏈上昭告天下，上述發行寫入與驗證取出的兩個機制主

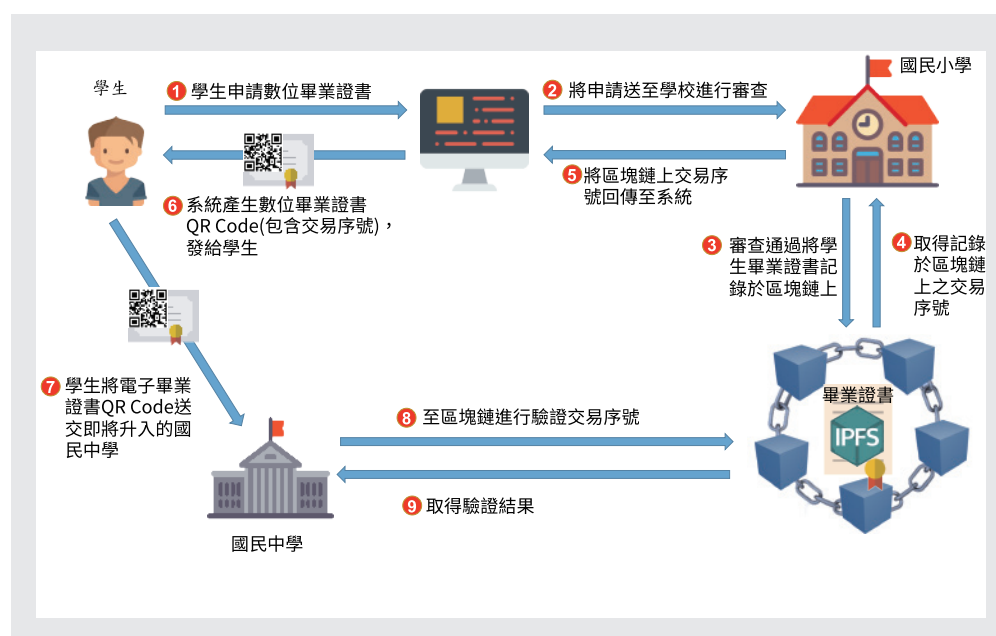


圖 3 數位畢業證書發行寫入、驗證取出步驟

要步驟如圖 3 所示。

未來可以進一步開發 App 讓學生管理自己的私鑰，驗證畢業證書的流程也可以加上向學生提出私鑰挑戰 Private Key Challenge，學生以透過此 App 回應挑戰，就可驗證該畢業證書所有權，更進一步做到 Proof of Ownership。

這樣的架構，把區塊鏈技術用到 Record Keeping 的實務上，一旦紀錄資料寫入區塊鏈，幾乎不可能被更動竄改，所以紀錄的安全性受到保障；而查詢資料的人可以用簡單快速的方式取得可信的資料，紀錄的可及性大幅提升，減少作業成本。

叁、實作成果

自去年底開始，國網中心開發團隊（圖 4）與市府同仁經過規格討論、節點架設、開發測試、介面調整等各種階段，在今年 6 月初提出了一個可以進入



圖 4 國網中心開發團隊

實際應用的版本，順利趕上小學的畢業季；在發展過程中教網中心阮志偉主任全力支持，而阮主任同時也是霧峰光正國小的校長，所以光正國小自然就成了此應用的示範學校。



圖 5 光正國小張貼「介紹區塊鏈數位畢業證書」海報

6月14日光正國小畢業當日，老師在典禮會場貼上了介紹區塊鏈畢業證書的海報（圖5），海報上有本屆19名畢業生的數位畢業證書驗證網址QR Code，臺中市政府蕭景燈資訊長於現場掃描QR Code，完成驗證，象徵性地頒發此畢業證書給畢業生（圖6）。

肆、閱讀認證寫入區塊鏈，讓數位公民管理自己的數位資產

有鑑於臺中市政府與國家實驗研究院國家高速網路與計算中心合作之「畢業證書區塊鏈PoC」於6月圓滿達成階段性任務，市政府資訊中心與教育局即刻思考如何將區塊鏈應用到更多教育場域。與學校關聯的應用即是由教育部資訊及科技教育司補助臺中市政府教育局進行的「臺中市線上閱讀認證系統」²優化專案。

² http://read.tc.edu.tw/reading_certificate/



圖 6 臺中市政府蕭景燈資訊長現場掃描 QR Code，完成驗證，象徵性頒發畢業證書

閱讀認證系統主要目的在提供學生一個得以進行閱讀理解能力測驗的平台，學生必須先閱讀過實體書籍，再進入平台回答與該書相關的問題，並在正確率超過 80% 以上，即取得該書的認證積分。隨著通過認證的書籍愈來愈多，學生也會取得相對應的閱讀鳥標章³，這些認證成績都可以視為學生學習過程累積的資產。不過，目前系統的登入帳號密碼必須藉由管理人員，以手動方式年年匯入，造成資料維護不易。同時，認證的資料是以資料庫方式儲存，若有遺失狀況發生，則學生的努力付之一炬。

閱讀認證系統的維護團隊（即是教育部委託臺中市政府教育局成立之「教育體系身分認證服務工作小組」）為了確保學生的閱讀認證資料可永久保

³ http://read.tc.edu.tw/reading_certificate/back_home_2.php

存、永久有效且無法竄改，因此著手擴充「畢業證書區塊鏈」的架構，藉區塊鏈技術來儲存學生的學習資料。同時為了也規劃建立一個臺中市政府教育局區塊鏈數位積點系統，將學習成就換算數位積點給予學生獎勵，在技術上即是一種 Asset Tokenization，這樣的區塊鏈不只是 Record Keeper 也是 Digital Currency。

閱讀認證系統將會是數位積點第一個運用的對象，學生在閱讀認證系統完成書籍認證並取得積分時，後端自動串接數位積點系統 API，將認證資料寫入區塊鏈之中，並產生一筆交易將獎勵的數位點數轉入學生的數位錢包。這些數位點數可以在錢包之間交換流通，累積的點數可以透由臺中市政府教育局的獎勵機制進行兌換，錢包內的點數兌換成實體獎品之後則直接銷毀。如此一來，這個點數機制間接促進學生的學習活動，達到更良好的學習成效。

現行有許多學習相關的網站也有虛擬點數設計，但是這些虛擬點數僅止於該網站內的運用，以舊的架構要實現跨站點數交換的成本太高並不可行。因此在閱讀系統優化專案運行順暢之後，工作小組預計規劃一個新的聯盟鏈，結合更多樣化的虛擬點數夥伴，讓區塊鏈分散共享的本質有最好的實踐。

伍、為數位原生代打造新世代的應用

臺中市區塊鏈的第一個試驗選擇教育學習場域，除了因為國民教育是地方政府的重要工作之外，也認知在學校階段的學生是熟悉各種數位工具的數位原生代（Digital Native）⁴，將區塊鏈應用引介至校園，引導學生了解這項科技，引發興趣與動機，藉以培養新世代數位國民。🌀

⁴ https://en.wikipedia.org/wiki/Digital_native



國發 動態

DEVELOPMENT

青年世代領航， 描繪 2050 國土空間 發展願景

國發會國土區域離島發展處

目前，我們居住的環境正面臨種種快速變遷與挑戰，如全球氣候變遷、能源危機、高齡少子化、互聯網與 AI 技術發展日新月異等，在在深刻影響全球社會與經濟發展的布局，我國空間發展的戰略方向勢必要提前思考因應。

展望 2050 年，國發會正在進行第四次國土空間發展策略規劃，從「氣候變遷與能資源」、「人口及社會變遷」及「科技技術」等三個發展面向，探討其將如何影響未來產業發展、生活及工作型態以及移動需求與方式，進而描繪出 2050 的前瞻願景，據以擘劃未來國土空間結構及城鄉發展型態，並提出各部門發展策略與機制，以引導國家建設及投資方向。

2050 年的國土空間發展願景充滿無限想像，而現在的學青世代正是未來主導城鄉發展的主體力量。因此，藉由青年學子們的朝氣活力與創意能量，共同勾勒 2050 臺灣國土空間發展樣貌，將有助於激發大家對未來的創新靈感與思考，讓青年參與國家政策規劃，也將使國家發展更增添活力。

未來城鄉是年輕人的城鄉

國發會自 106 年起，即邀請全國空間規劃相關系所師生參與未來城鄉發展規劃，今（107）年更擴大規模，共有包括國立臺北大學（都市計劃研究所）、國立臺北科技大學（建築系暨建築與都市設計研究所）、臺北市立大學（城市發展學系）、中國文化大學（都市計劃與開發管理系）、國立臺灣大學（建築與城鄉研究所）、逢甲大學（土地管理學系、都市計畫與空間資訊學系）、國立成功大學（都市計劃學系）、國立中山大學（公共事務管理研究所）、國立臺東大學（公共與文化事務學系）、國立金門大學（都市計畫與景觀學系）等 10 校 11 系所熱情投入，透過學校專業課程，結合跨校系工作坊的對談交流，年輕學子們以臺灣各地方進行案例模擬，具體描繪出 2050 年



陳主委美伶出席「2050未來城鄉發展」跨校規畫成果聯展開幕致詞。

我國城鄉環境的各種意象，涵蓋資源循環、低碳、未來建築、綠建築、無人車、人工智慧等主題，展現出繽紛多元、充滿想像力的精彩規劃成果。

國發會於 107 年 6 月 30 日起連續三天，在臺北火車站 1 樓多功能展演廳舉辦「2050 未來城鄉發展」跨校規劃成果聯展，從「共融」、「共生」、「共享」三個面向探討未來城鄉規劃，共同發想國土未來願景。

陳主委美伶特別於開幕式中指出，未來的城鄉是年輕人的城鄉，未來的國土空間發展需要年輕一代的創意去想像。2050 年臺灣人口將少於 2000 萬人，同時面臨高齡化及區域發展差距的課題，因此，國發會除了國土規劃外也正積極推動地方創生的相關政策；另外，現在科技發展瞬息萬變，我們更應該要深入了解與因應科技發展 ABCDE 五大趨勢，即人工智慧（AI）、



陳主委美伶參觀「2050未來城鄉發展」跨校規劃成果聯展。

區塊鏈 (Blockchain)、雲端技術 (Cloud)、數據 (Data) 及生態系統 (Ecosystem) 等五個面向，這些對國家國土空間發展與布局都將會有深切的影響。

開啟通往未來城鄉的一扇窗

本次跨校成果聯展是經過 3 場的工作坊、2 場的座談會以及整個學期師生們的創意發想，所描繪出未來 2050 年我國城鄉環境的各種意象，成果斐然且圓滿成功，也為我國國土空間發展規劃注入年輕的朝氣與活力，開啟通往未來城鄉的一扇窗。🌀



「2050未來城鄉發展」跨校規劃成果聯展開幕合影。

出席APEC 經濟委員會 第2次會議(EC2) 暨結構改革高階官員會議

國發會綜合規劃處

2018年APEC 經濟委員會第2次會議(EC2)於8月14至17日在巴布亞紐幾內亞(以下簡稱巴紐)首都莫士比港召開，國家發展委員會(以下簡稱國發會)為我國參與APEC 經濟委員會(Economic Committee, EC)之總協調窗口，爰本次會議由國發會綜合規劃處張處長惠娟偕同本會資訊管理處、法制協調中心，以及法務部法律事務司等單位代表共同出席。

2018年APEC 主辦會員體巴紐所設定主題為「掌握包容性機會，擁抱數位未來」(Harnessing Inclusive Opportunities, Embracing the Digital Future)，並列出包括「透過結構改革以強化包容性成長」等三大優先領域。而EC係APEC 推動結構改革之重要推手，本年為盤點「APEC 結構改革更新議程(Renewed APEC Agenda of Structural Reform, RAASR) 2016-2020」之推展成果，巴紐於本次EC2 會議後，在8月16至17日接續召開「結構改革高階官員會議(High-Level Structural Reform Officials' Meeting, HLSROM)」。茲就本次EC2 及HLSROM 會議重要結論摘要說明以下：

壹、EC2會議

■ RAASR期中成果盤點

APEC 政策支援小組 (Policy Support Unit, PSU) 就 RAASR (2016-2020) 期中檢視成果進行報告，整體而言，APEC 會員體雖在創新及生產力提升等方面有所進步，惟其他如基礎建設、財政與社會政策、擴大社會各群體之經濟參與 (尤其是青年就業) 等領域，尚須賡續強化推動。我方張處長惠娟於會中發言肯定 PSU 就 RAASR (2016-2020) 期中檢視成果之報告，感謝巴紐



國家發展委員會出席APEC經濟委員會第2次會議 (EC2) 代表團進場情形。

召開 HLSROM，並表示 APEC 各會員體可利用此機會盤點 RAASR 自 2016 年實施以來之進展，未來希望能與和我方有相同優先政策領域之會員體合作，推動具體提案，以共同對 RAASR 執行作出貢獻。



本會參與2018年APEC經濟委員會第2次會議（EC2）情形。

此外，經商便利度（Ease of Doing Business, EoDB）係現階段 EC 結構改革優先領域工作計畫之一，現行 APEC 第 2 期 EoDB 行動計畫（2016-2018）將於本年底執行屆滿，至 2017 年底該計畫五大指標（1. 開辦企業；2. 建築許可；3. 獲得信貸；4. 跨境貿易；5. 執行契約）整體進展為 7.3%，較預期為高，其中進展最顯著者為「獲得信貸（18.1%）」，其次為「開辦企業（11.8%）」。另該計畫主導會員體美國於會議中，呼籲各會員體就預計將於 2020 年展開的新一期 EoDB 指標調整進行廣泛研議。

■ APEC 經濟政策報告（AEPR）

由主導會員體紐西蘭發表 2018 年 AEPR — 結構改革與基礎建設之研究成果，並提出各會員體個別經濟體報告（Individual Economy Report, IER）。依據該報告之結論，APEC 區域內基礎建設面臨的挑戰主要為：缺乏偏遠地區包容性與連結性、對優質數位基礎建設的迫切需求，以及缺乏良好的制度結構等。

巴紐與智利則針對 2019 年 AEPR 主題提出初步構想，建議主題為「結構改革與數位經濟」，相關建議將提交總結資深官員會議（Concluding Senior Officials' Meeting, CSOM）及部長級年會（APEC Ministerial Meeting, AMM）核可。另 2019 年 APEC 主辦會員體智利於會中表示願主導 2019 年 AEPR 撰擬小組，我方亦於會後表達加入該小組之意願。

■結構改革及包容性成長

EC 依據 2015 年結構改革第 2 次部長會議指示、2016 年 APEC 經濟領袖宣言，以及 2017 年「APEC 經濟、金融、及社會包容性行動議程」（APEC Action Agenda on Social, Financial, and Economic Inclusion），研擬一套結構改革與包容性成長政策架構，紐西蘭於本次會議中提出該政策架構草案。

另 PSU 針對貿易、政策與包容性所做研究指出，經世界銀行對 170 個經濟體之長期觀察，全球化與國際貿易雖可能影響與進口產品相互競爭部門的就業，但以保護國內就業為名施行保護主義，實則將對經濟體國內工作機會、實質薪資與經濟成長造成負面影響，因此正本之道，應致力發展人力資本、社會包容性政策，並提升基礎建設、金融包容性，以及貿易與區域整合等措施，積極透過結構改革以促進包容性。

我方張處長惠娟發言感謝 PSU 對於結構改革與包容性成長所做的詳實的研究，並表示如 PSU 研究所示，全球化與貿易不只帶來經濟發展的好處，也對社會包容性產生影響，政府面對經濟與社會不平等議題的挑戰也越來越大。EC 作為 APEC 政策討論的平台，應持續探入探討此議題。

■APEC 網路與數位經濟路徑圖（APEC Internet and Digital Economy Roadmap, AIDER）

由 EC「非正式路徑圖小組（Informal Roadmap Group, IRG）」（我方亦為 IRG 成員）的主導會員體澳洲，報告 IRG 對於 EC 未來執行 AIDER 之初步

評估結果，該報告中依 IRG 調查票選結果，建議 EC 優先執行路徑圖 11 項關鍵領域中之前 3 項：發展網路及數位經濟整體性政府政策架構、提倡網路及數位經濟監理方法之調和與合作、提升網路及數位經濟的包容性。另 IRG 將於休會期間撰擬 EC 2019 年執行路徑圖之工作計畫，並預計提交 CSOM 採認。

我方張處長惠娟發言首先感謝澳洲領導 IRG，並表示先前在「網路經濟特別指導小組（Ad Hoc Steering Group on the Internet Economy, AHSGIE）」已針對數位經濟有十分熱烈的討論，反映出此議題之複雜程度，因此有關路徑圖後續執行的協調與監管，建議應由更高位階的 APEC 組織來主導進行，再向資深官員會議（Senior Officials' Meeting, SOM）報告；EC 是 APEC 的政策討論與規劃平台，關於 AIDER 所提出的 11 個關鍵領域中，我方認為不該只專注在票選出來的 3 個優先關鍵領域，應抱持開放的態度，在 EC 廣泛思考與討論如何面對數位經濟所帶來的挑戰。張處長並表示感謝及認同 OECD 所提目前數位經濟監管方式之簡報，現今在數位時代，政府應思考如何善用新興科技精進公部門治理，例如利用分散式帳本技術（如區塊鏈或 IOTA 等）應用於公共治理。貿易暨投資委員會（Committee on Trade and Investment, CTI）已經在探討如何利用區塊鏈來促進跨境貿易等，EC 也應跳脫既有的框架內容，納入更多新議題進行討論。

貳、HLSROM會議

本次 HLSROM 會議採認 EC 所提交之 RAASR 期中成果盤點及結構改革及包容性成長政策架構，並探討結構改革之未來新興議題，如數位經濟、連結性、包容性、及基礎建設等，以及展望 2018 至 2020 年如何進一步執行 RAASR 的工作，為 APEC 的結構改革目標再跨出重要一步。

■ RAASR個別行動計畫（Individual Action Plan, IAP）

我方亦於會議中由綜規處黃科長仿玉進行簡報，分享我方 RAASR IAP 中，有關競爭政策、法制環境、金融包容性、微中小企業國際化、以及提升婦女經濟參與等領域在 2016 年至 2018 年間之執行進展。

■ 結構改革新興議題－數位經濟

有關數位經濟議題的討論，我方張處長發言表示，如同 OECD 簡報提及，破壞性創新科技不只帶來數位經濟的機會，但也對政府施政帶來挑戰。例如：政策制定經常趕不上技術發展的腳步，不合時宜的法規可能阻礙創新的經濟活動。除了經濟課題，政府也須採取必要的因應措施，處理就業與教育等社會層面的問題，如：加強職能訓練，或從基礎教育即開始培訓數位時代所需技能等，降低對社會面的衝擊。另，不只企業必須數位轉型升級以更有效地使用



本會參與2018年APEC結構改革高階官員會議（HLSROM）情形（照片來源：APEC官網）。

新資通訊工具，對政府而言，如何利用創新科技優化政府決策及治理，同樣也是新興挑戰。為討論可行解決方案，EC 應與 APEC 各論壇、次級論壇，如電子商務推動小組（Electronic Commerce Steering Group, ECSG）及電信工作小組（Telecommunications and Information Working Group, TELWG）等協力，並應積極與 EC 已合作多年的 OECD 等國際組織共同合作，討論如何因應數位轉型的課題，此對 APEC 各會員體均是學習過程，對於破壞性創新科技帶來的轉變，我們的心態應更加開放。

叁、結語

APEC 為因應近年來全球經貿情勢的快速變遷，現正積極推動結構改革，以強化 APEC 區域整體之投資環境與經商便利度，此與我政府施政主軸「加強投資臺灣及落實結構改革，以全力提振國內經濟」實相互契合呼應。國發會身為協調我國各部會參與 EC 事務之主責單位，未來將秉持一貫之積極、主動態度，持續精進相關發展課題研析，並積極參與區域間倡議，以強化我國國際參與及全球鏈結。🌐

2018年APEC企業諮詢 委員會(ABAC)數位創新 論壇(DIF)

國發會綜合規劃處

APEC 企業諮詢委員會 (APEC Business Advisory Council, ABAC) 於今 (2018) 年 7 月 19 至 20 日在臺北國際會議中心盛大舉辦「數位創新論壇」(Digital Innovation Forum, DIF)，全球重量級數位創新領袖共襄盛舉，為近期我國所辦理最高規格之國際論壇。國發會為我國參與 APEC 之重要政策幕僚，相當重視此次 DIF 活動，除在籌辦過程中予以大力協助外，國發會陳主任委員美伶亦應邀出席官方晚宴並致詞。

本次 DIF 是由我國 ABAC 與今年 APEC 主辦會員體巴布亞紐幾內亞 ABAC 合作辦理，針對全球數位創新產業發展之現況與趨勢，從「破壞性創新對人類生活的影響」、「科技發展帶來的商業機會」、「全球社會因應數位化所面臨的轉型議題」三大主題解讀數位創新之全球趨勢脈絡。本次論壇邀集全球重量級數位創新領袖與會，包括愛沙尼亞前總統 Toomas Henrik Ilves、維基百科創辦人 Jimmy Wales、3D 機器人公司執行長 Chris Anderson、日本瑞穗銀行總裁林信秀及 Gogoro 執行長陸學森等。

陳主委於致詞時表示，APEC 作為亞太區域經濟整合的重要平台，也是我國目前參與最重要的國際組織之一，我國曾以 APEC 數位機會中心 (APEC Digital Opportunity Center, ADOC) 協助 APEC 會員體提升數位經濟能力並



DIF邀請世界首位公民機器人索菲亞（Sophia）與我方ABAC代表詹宏志先生、2018年ABAC副主席 Wayne Golding共同擔任開幕嘉賓。

縮短數位落差，成果廣受好評，為我國在 APEC 之重要貢獻，今我國與巴紐共同辦理 DIF，同樣亦為我國對 APEC 區域貢獻之見證。此外，陳主委感謝並肯定我國目前 3 位 ABAC 代表：網路家庭（PChome）國際資訊股份有限公司詹宏志董事長、義美食品股份有限公司高志尚董事長及王道商業銀行駱怡君副董事長在 ABAC 之積極參與，特別是詹董事長投入籌辦 DIF 之努力。

陳主委續指出，DIF 所討論的議題，包括掌握數位機會、發展數位經濟、帶動數位轉型，並及早因應隨之而來的挑戰，與我國刻正推動之整體國家發展重要政策相符。在數位經濟時代下，政府擴大國內投資的五大路徑為「A、B、C、D、E」，也就是強調 AI（人工智慧）、Blockchain（區塊鏈）、Cloud（雲端）、Data（數據）、Ecosystem（產業生態系）的重要性，以帶動創新產業發展，將強化我國產業在全球供應鏈的優勢，打造臺灣成為數位國家、智慧島嶼；另一方面，政府亦密切關注數位科技與應用的發展，對於法規環境、經濟活動、社會關係與人民生活的影響，並確保有越來越多創新的數位產品與服務可協助解決高齡化、健康照護落差、節能等社會與環境議題。



國發會陳主委美伶出席DIF晚宴致詞。

本次論壇除了讓世界看見臺灣，國內政府部門及企業亦可自與會的數位創新專家所提供之前瞻見解借鏡，例如：

—愛沙尼亞前總統 Mr. Toomas Hendrik Ilves 在專題演講中分享：「數位政府最核心的價值鏈始於電子身分證（Digital Identity），透過每個人經認證的電子簽名來行使其公民權利並接受公共服務，如：電子投票、電子稅務服務、商業登記等，以及建立一個公開、透明、受人民信任的資訊保護措施，同時強化私部門在此過程中之參與，以達到數位治理的目的。」

—維基百科創辦人 Mr. Jimmy Wales 在專題演講中提到：「未來科技創新



DIF為近期我國所辦理最高規格之國際論壇，吸引國內外各界菁英與會（照片來源：2018數位創新論壇）。

必定往更開放、透明的方向發展，創新生態系的新模式將大幅改變未來十年的科技趨勢，而每個人都具備參與此創新生態系並做出改變的能力，應以開放的心態來面對未來世界可能的轉變。」

ABAC 向來為各會員體企業界於 APEC 場域發聲的重要平台，係由 21 個 APEC 會員體領袖指派本國 3 位來自大、中、小型企業之企業家所組成，代表亞太區域之企業界，每年向 APEC 領袖提出政策建言，並在 APEC 經濟領袖會議期間進行政策對話。ABAC 今年以「促進社會和諧的數位化與創新」(Digitalization and Innovation - Advancing Social Harmony) 為主題，同時為因應數位浪潮對於產業與人才的衝擊，設立數位創新工作小組 (Digital and Innovation Working Group, DIWG)，邀請我國在科技及發展電子商務上具有成功經驗之詹宏志代表擔任第一任主席，舉辦本次 DIF 將為本年最重要的工作成果。🌐

臺灣新創勇闖2018 香港RISE，再傳捷報

國發會產業發展處

近年政府積極推動創新創業，從資金、法規、人才、國際鏈結等面向著手，打造完善的創新創業生態系。其中，協助我國新創鏈結海外資源與人脈，提高臺灣創新創業的國際能見度，更是國家發展委員會（以下簡稱國發會）努力的重點。

今（2018）年7月，國發會與臺灣新創競技場（Taiwan Startup Stadium, 以下簡稱TSS）連續第3年率領新創團隊赴香港參加RISE活動，以設置臺灣展區（Taiwan pavilion）的方式，打造國家品牌形象，透過有系統地對外行銷，讓國際看見臺灣創新創業的豐沛能量。

RISE是由國際知名科技新創盛會Web Summit在亞洲創立的活動品牌，自2015年在香港舉辦，今年邁入第四屆。根據RISE官網揭露，今年7月10日至12日為期三天的活動，吸引超過100個國家、近15,000位與會者（其中七成為公司管理階層）、750家新創團隊參加，並有超過350名講者，12名世界級演講嘉賓，包括Microsoft總裁Brad Smith、Amazon技術長Werner Vogels、Line執行長出澤剛及以太坊共同創辦人Joseph Lubin等。活動合作夥伴包括Amazon、Facebook、Google、IBM、AWS等企業，TSS也是其中之一。

今年，TSS 再度以「#TaiwanRocks」國家品牌參展，並在 RISE 活動前三個月，以「Rock the Mic Asia」為主題，與報名 Infinity Ventures Summit（日本）和 Techsauce Global Summit（泰國）的新創團隊一起進行徵選。為了搶進 RISE 的免費門票，團隊必須在 2 分鐘內以全英文闡述生意經、展現科技魂以及強烈的企圖心。經過一番激烈較勁，最後選出 8 組新創團隊進駐 RISE 展區，領域涵蓋人工智慧、數位教育、金融科技、共享經濟等。

這 8 組團隊分別為：FRM（粉絲關係管理平台）、Clef Technology（以聲波進行工廠管線漏氣預測）、Hahow 好學校（結合線上課程與募資平台）、PiStage（動畫製作與建置軟體）、ReCactus（製作流行短影音的 App）、STO



TSS帶領8組新創在香港RISE展區合影。

MAP（室內地圖應用及線下大數據分析平台）、Addweup（提供剩餘外幣儲值電子錢包或捐贈平台）、Screea（推薦美食之共享經濟 App）。

今年 RISE 的展區安排與往年差異不大，臺灣展區也持續以活潑的主視覺及整體品牌設計，營造臺灣新創的活力形象。有了前幾年的經驗，TSS 已發展出一套系統性的教戰攻略，不僅在行前提供全英文培訓，更安排團隊真槍實彈的 Pitch 演練，就其簡報內容、演說重點、用字遣詞以及行銷方式給予許多建議，以加強新創團隊的實力。此外，在 RISE 活動期間，TSS 也為新創團隊積極引介創投或企業資源，並提醒團隊專注於產品展示與自我行銷，把握機會



Screea創辦人William向與會者解說產品及服務內容，互動熱絡。

認識媒體與潛在投資者，爭取更多曝光與合作。雖然活動行程緊湊，許多團隊仍爭取時間與客戶洽談業務，充分展現拓展國際市場的企圖心。

除了展區以外，Pitch 大賽也是 RISE 的重要活動之一，更是新創團隊最快速的行銷管道。來自世界各地的團隊，在台上以 4 分鐘的時間，宣揚產品優勢、商業模式及市場獨特性，並由國際知名企業、創投等組成評審團，經過重重篩選，於活動最後一天在主舞臺進行 Final Pitch。TSS 所帶領的新創團隊，在去年由 Pointimize（點數旅遊搜尋引擎）奪下冠軍之後，今年由 ReCactus 代表臺灣，擊敗亞洲其他 7 組強隊衛冕成功。負責上台 Pitch 的



ReCactus CEO Bernard代表臺灣在RISE奪下Pitch大賽冠軍。

Bernard Tan 在比賽前一晚坦言，背負著臺灣團隊奪冠的壓力，心情非常緊張。所幸最後在平日堅實的訓練下，不負眾望再創佳績。

國發會與 TSS 自 2015 年開始帶領新創團隊出國參展，目前足跡已遍及美國 TechCrunch Disrupt、Collision，日本 Slush Asia、新加坡 Echelon、泰國 Techsauce 及香港 RISE 等。除了參與國際新創展會外，後續也促成不少業務合作與投資，例如 FunNow（旅遊娛樂即時預訂服務）在去年參加 RISE 後，逐漸打開香港市場，並在今年 8 月完成 500 萬美元募資，將進軍馬來西亞及日本。此外，Rooit（匿名聊天交友服務）也在 TSS 的培訓下，在今年入選位於新加坡、由國際知名加速器 Techstars 與日本樂天合作的加速器計畫。

這些優秀的成績，不但代表臺灣新創實力堅強，也顯示在政府與民間共同努力下，臺灣的新創生態環境逐步完善，新創發展日益蓬勃。未來，我們希望能促成更多新創成功案例，並協助這些優秀的新創團隊邁向國際市場，進一步提升臺灣創新創業的國際能見度。🌐

2018 年景氣指標及對策信號 檢討與修正說明

國發會經濟發展處

本會景氣指標及對策信號自 1977 年開始公布，廣為各界使用。其中，景氣指標與對策信號分別前於 2013 年修訂¹，本次（2018 年）修正作業主要考量國內經濟結構轉變、個別統計指標反映景氣循環能力有所鈍化，加以部分指標中止發布等因素，特進行通盤檢討修正，期能精確、即時反映景氣概況。

壹、修正過程

一、由本會先自行研析、檢討

由本會自行研析、檢討，逐一檢視指標與燈號表現，並剔除循環對應性不佳之構成項目，重新挑選適當構成項目替代。

二、就相關問題委託研究

針對部分特定議題委託學者專家進行研究，藉此精進構成項目選取與指標編製方法，強化景氣指標系統對景氣判斷的精確度。

¹ 景氣指標分別於 1978 年、1987 年、2007 年及 2013 年經過 4 次修訂；景氣對策信號則分別於 1978 年、1984 年、1989 年、1995 年、2001 年、2007 年及 2013 年歷經 7 次修訂。

三、邀集學者專家、政府機關與民間學術單位共同研商

就檢討後初步修正結果，邀請學者專家、政府機關代表共同檢視，並依其建議進一步完善景氣系統。

四、修正結果提報委員會議，並進行6個月試編

將修正結果提報國家發展委員會議，決議新版景氣指標及燈號自 2018 年 2 月起進行為期 6 個月試編。

五、決議新版自2018年8月27日正式啟用、銜接

歷經 6 個月試編結果顯示，修正後景氣指標與燈號表現良好，更可精確反映景氣概況。有鑑於半年的試編結果穩定，有效精進景氣波動掌握力，故委員會決議自 8 月 27 日起啟用新版景氣系統。

貳、修正結果

一、景氣指標

景氣指標包括領先、同時、落後指標，本次修正重點在於重新檢視指標及其構成項目之景氣循環對應性，至編製方法仍沿用 OECD 統計方法編製合成景氣指標。針對部分循環對應性不佳之構成項目，考量經濟重要性、循環對應性、統計充足性等因素，測試、篩選多項經濟數據後，予以替換。

(一) 領先指標

既有領先指標部分構成項目隨經濟結構變遷，已逐漸喪失對景氣的預判能力；加以部分統計指標因調查作業因素而中止發布，影響領先指標之編製。

1. 修正重點

一以「外銷訂單動向指數（以家數計）」替代「外銷訂單指數」：「外銷

「訂單指數」因發布機關中止發布，故予以剔除，並以可以反映外銷廠商預期下個月訂單變化的看法之「外銷訂單動向指數（以家數計）」替代。

一以「建築物開工樓地板面積」替代「核發建照面積」：考量核發建照具 6 個月的時效性，使核發建照與實際開工具有一定程度落差，或存在開工的不確定性；而「建築物開工樓地板面積」對應景氣循環具穩定領先性。

一至其他構成項目表現良好，可用來預測未來景氣變動，予以沿用。

2. 修正結果（詳見圖 1）

一新、舊領先指標趨勢方向一致，但新領先指標更具領先性。

一自 2000 年以來平均領先景氣高峰 6 個月，領先谷底 2 個月，整體平均領先 4 個月，較舊版提高 1 個月。

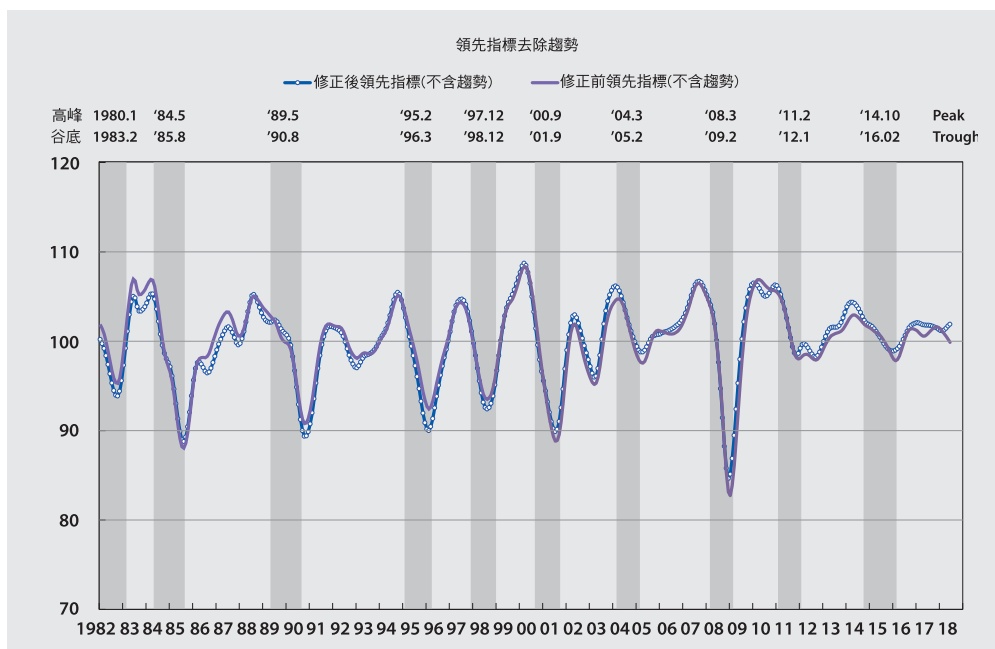


圖 1 修正前後領先指標比較

(二) 同時指標

依據學者專家及相關部會研商會議之決議，同時指標及構成項目對景氣循環的對應性仍佳，且可同步反映景氣循環波動，同意沿用維持不變。

(三) 落後指標

既有落後指標部分構成項目落後期數過長，且期數接近平均收縮期持續期間（15 個月），有必要加以修正。

1. 修正重點

一刪除「工業及服務業受僱員工人數」：因資料及時性稍差，且與同時指標構成項目「非農業部門就業人數」之意涵重疊，擬以「失業給付申請人數」替換，試編發現該項目與「失業率」若併存於落後指標，將加重短期失業波動的影響，故剔除「工業及服務業受僱員工人數」並無替代項目。

一以「全體金融機構放款與投資」取代「全體貨幣機構放款與投資」：考量全體金融機構涵蓋範圍包括全體貨幣機構（中央銀行及本國銀行等其他貨幣機構），以及信託投資公司與人壽保險公司，涵蓋範圍較廣，更具代表性。

一以「製造業存貨價值」取代「製造業存貨率」：原「製造業存貨率」因落後平均期數長達 12 個月，改以落後性較佳之「製造業存貨價值」替換。

2. 修正結果（詳見圖 2）

一大幅縮短反映已發生景氣之所需時間。

一自 2000 年以來平均落後景氣高峰 7 個月，落後谷底 7 個月，整體平均落後 7 個月，較舊版指標縮短 2 個月。

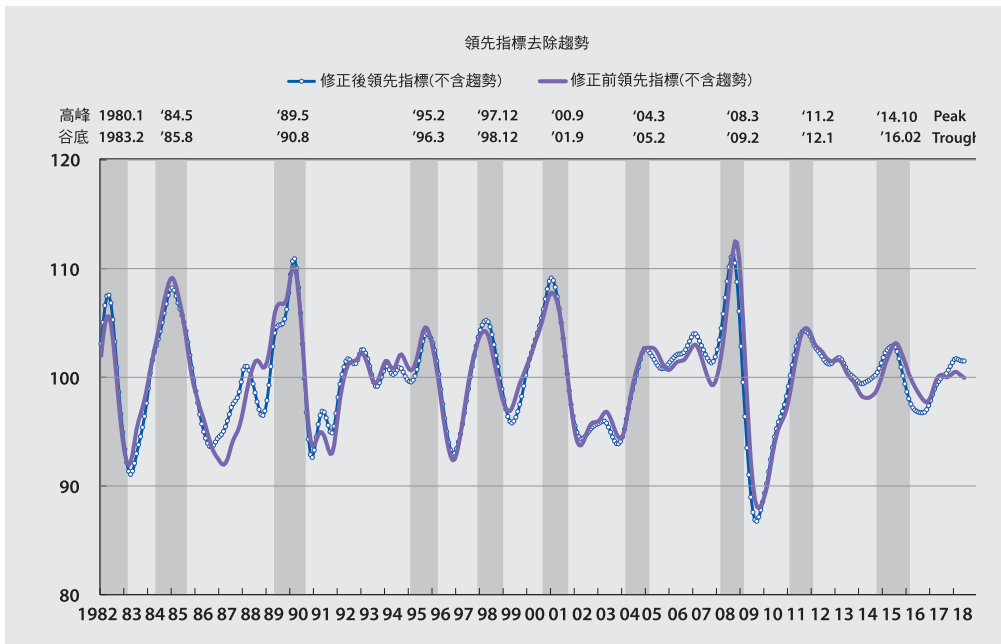


圖 2 修正前後落後指標比較

二、景氣對策信號之修正

景氣對策信號（又稱景氣燈號）係由與景氣波動密切相關之重要經濟指標，綜合編製而成，藉由 5 種不同燈號（紅燈、黃紅燈、綠燈、黃藍燈、藍燈）變化，提供景氣波動信息，現已成為各界判斷景氣榮枯之重要參考依據。

（一）構成項目維持不變

考量景氣系統的一致性，經與專家學者研商會議結果，九項構成項目維持不變。

（二）修訂檢查值

1. 本次修正根據 2000 年至 2017 年（涵蓋至少 4 次景氣循環）各構成項目年變動率為觀察樣本，以 Bootstrap 統計方法，並參酌學者專家對未來景氣判斷，綜合研訂。

2. 經重新檢視個別項目之燈號檢查值，修訂後，黃紅、綠燈之檢查值門檻普遍往下移，藍燈上限值則往上移。

(三) 修正結果 (詳見圖 3)

修正後景氣燈號更能反映景氣動向。2000 年以來，綜合判斷分數與經濟成長率維持高度相關；而近五年之相關性 (2013.1 ~ 2018.6)，則由 0.82 提升至 0.85。

叁、結論

- (一) 修正後景氣指標系統能更精確反映景氣概況，有助於各界判斷景氣變化。
- (二) 新版景氣指標與對策信號，於 2018 年 8 月 27 日發布 7 月景氣概況時啟用、銜接。

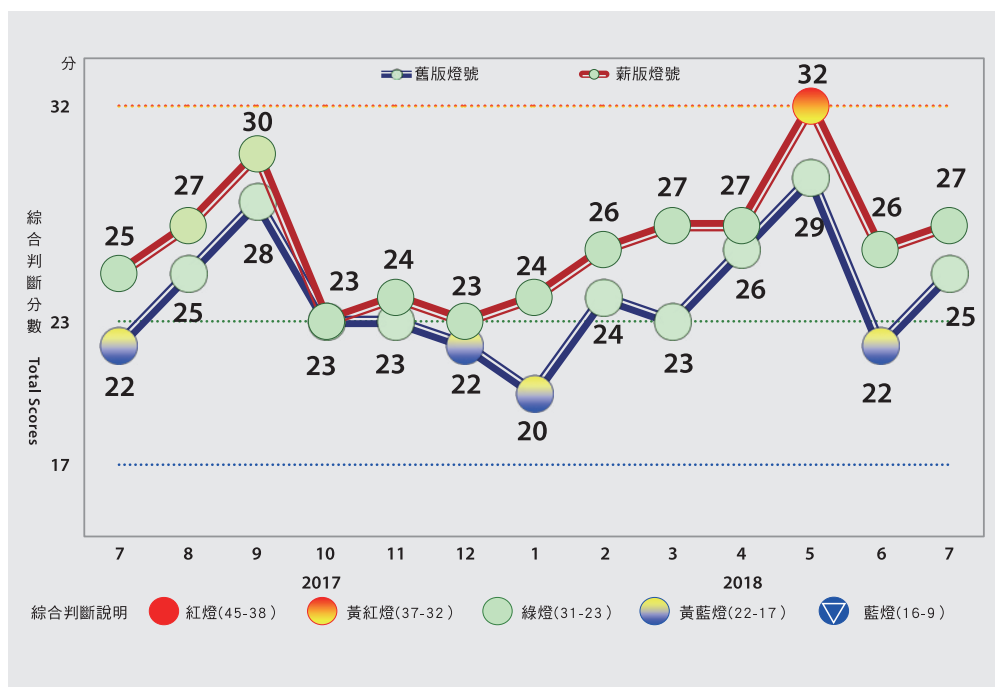


圖 3 修正前後燈號比較

中華民國人口推估 (2018 至 2065 年)

國發會人力發展處

人口為國家構成的基本要素之一，為了解我國未來人口數量及年齡結構之長期變動趨勢，以做為政府機關擬定人口、教育、勞動力、產業發展、都市住宅、社會服務及醫療服務等相關政策之規劃依據，本會每 2 年根據最新戶籍人口統計資料，更新人口推估結果，最新一期「中華民國人口推估（2018 至 2065 年）」報告，業於本（2018）年 8 月 30 日上網公布，供各界參考運用。本次推估結果重點摘要如下：

壹、推估方法及假設情境

我國人口推估係採用國際間慣用之「年輪組成法」，並輔以專家學者對出生、死亡及國際遷徙等相關參數之設定等做法進行。由於出生是影響未來人口數及年齡結構變化最關鍵之要素，爰參照國際間主要作法，將總生育率設定高、中、低 3 種假設情境，亦即假設總生育率於 2040 年分別達到 1.5 人、1.2 人及 0.9 人，代表回升、微升及持續下降 3 種趨勢，而死亡及遷徙則設定單一假設，從而形成人口推估之高、中、低推估結果。

貳、總人口成長趨勢

在生育率達 1.2 人之中推估假設情境下，我國總人口將於 2021 年達最高峰 2,361 萬人，惟若總生育率能反轉回升，在 2030 年達成 1.4 人之政策目標，並於 2040 年提升至高推估之 1.5 人水準，則人口成長將可持續至 2027 年，最高峰達 2,372 萬人。在低、中、高推估三種不同假設情境下，2065 年總人口數將降為 1,601 萬至 1,880 萬人之間，與 2018 年相比，約減少 2 至 3 成。

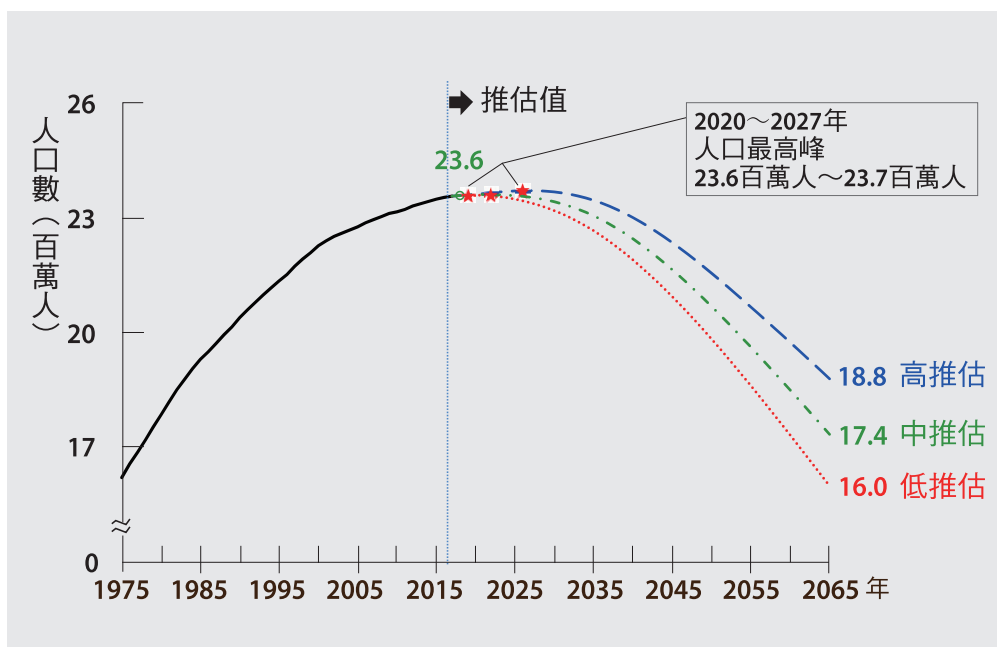


圖 1 總人口成長趨勢——高、中、低推估

參、人口年齡結構趨勢

過去我國生育率長期持續下降，使育齡婦女人數隨之減少，再加上晚婚使得年齡偏高齡化，未來即使生育率提升，出生數仍將持續減少，少子高齡化趨勢仍將持續，以下為中推估結果。

在 0-14 歲幼年人口部分，未來幼年人口數將持續下降，預估 2030 年將減少至 268 萬人（減 12.1%），至 2065 年將減少至 159 萬人（減 48.0%）。

15-64 歲青壯年人口（又稱工作年齡人口）則自 2015 年達最高峰後開始下降，目前占總人口比率仍大於 66.7%，尚處人口紅利階段，惟預估此人口紅利將於 2027 年消失，至 2065 年則減少為 862 萬人（減 49.6%）。

在高齡化趨勢方面，我國於本年進入高齡社會，預估 8 年後（2026 年），我國老年人口占比將超過 20%，成為超高齡社會的一員，高齡化速度較歐、美、日等國為快。預估 2065 年老年人口將增至 715 萬人（增 108.4%），占總人口比重達 41.2%。在此趨勢下，青壯年人口扶養負擔亦隨之增加，總扶養比（每百名青壯年人口所需撫養之依賴人口數）由 2018 年 37.9 上升至 2065 年 101.4，屆時依賴人口數將超越青壯年人口。

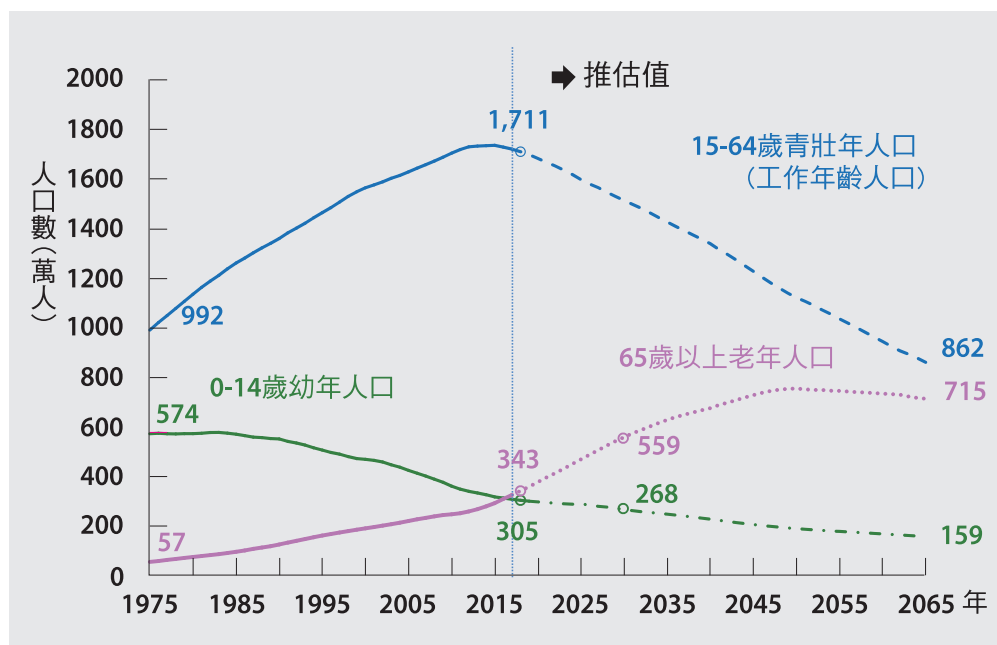


圖 2 三階段人口趨勢——中推估

肆、人口重要指標大事紀

- 2015 年 15-64 歲工作年齡人口數達最高峰，2016 年開始下降。
- 2017 年 2 月起 65 歲以上高齡人口數超越幼年人口
- 2018 年 1-7 月出生數較前一年同期減少 5,800 多人，3 月高齡人口占比超過 14%，正式邁入「高齡社會」
- 2020 年 死亡人數超過出生人數，自然增加率由正轉負
- 2022 年 總人口開始負成長
- 2026 年 高齡人口占比超過 20%，開始進入「超高齡社會」
- 2027 年 15-64 歲工作年齡人口占總人口比率開始低於三分之二，人口紅利結束
- 2034 年 年齡中位數達 50.1 歲，代表全國每 2 人中即有 1 人超過 50 歲
- 2036 年 18 歲（大學入學年齡）人口開始持續低於 20 萬人
- 2054 年 總人口開始低於 2,000 萬人

註：本表所列數值 2020 年以後為中推估結果。

本報告於本（2018）年 8 月 30 日第 59 次國家發展委員會議中報告，本會陳主任委員美伶指出，行政院本年在地方創生政策中，即訂定將總生育率在 2022 年提升至 1.25 人，2030 年提升至 1.4 人，並以總人口不低於 2,000 萬人做為施政目標，以達到國家「生生不息」、「均衡臺灣」。陳主任委員並強調，本報告應做為政府政策規劃之依據，針對可預見之人口結構變遷及早準備，預為因應，除強化刻正推動之少子女化對策，擴散其政策效益外，面對我國相對嚴峻之人口結構問題，臺灣須開放心胸朝「多元民族國家」邁進，營造友善移民環境，並進行相關配套措施規劃。此外，在數位經濟時代下，如何應用新科技提高國人生產力，降低人口結構變遷之衝擊，以及面對人工智慧取代人力之威脅，如何強化國人技能培訓，亦為政府須積極面對之課題。🌀

歐盟一般資料保護規則 (GDPR) 研討會

國發會法制協調中心

歐盟一般資料保護規則 (General Data Protection Regulation, GDPR) 已於今 (2018) 年 5 月 25 日全面施行，建立了一套嚴格的個人資料保護法制架構，其廣泛的影響力，已促使許多國家重新檢視個人資料保護相關法規。另由於 GDPR 的適用範圍可能擴及歐盟境外企業，且於跨境傳輸方面採取「原則禁止、例外允許」的模式，也引起對於「適足性認定」議題 (係指倘第三國或地區個人資料保護程度達到 GDPR 規範的標準，進而取得歐盟適足性認定資格，則該國或地區即可自由與歐盟間進行個人資料跨境傳輸) 的關注，據悉近期日本即將取得歐盟的適足性認定，而韓國亦積極洽談中，我國對此當不能置身事外。

面對 GDPR 的衝擊與影響，行政院賴院長已於今年 5 月 24 日院會指示各部會應積極協助提供所轄產業相關輔導與諮詢服務，並責成國家發展委員會 (下稱國發會) 成立「個人資料保護專案辦公室」，作為協調與整合各部會的平臺，並統籌辦理因應 GDPR 相關事宜。

國發會遂於今年 7 月 4 日成立「個人資料保護專案辦公室」，除於官網設立 GDPR 專區並適時更新相關資訊外，為加強公部門對於 GDPR 的瞭解，國發會亦於今年 8 月 22 日舉辦「歐盟一般資料保護規則 (GDPR) 研討會」，邀

集中央、地方政府與專家學者共同探討歐盟 GDPR 施行的影響以及政府因應作為與調適方向。

國發會陳主委於本次研討會開幕致詞時表示，數位經濟已成為全球不可逆的發展趨勢，不論在智慧政府或數位社會的發展上都需要進行大數據運用，然而卻也對個人資料的保護帶來相當衝擊，因此必須透過個人資料保護意識的提升、透明機制的落實，才能產生信賴度，進而促進資料流通。

陳主委並說明，臺歐經貿關係密切，為協助企業對跨境傳輸的需求，國發會已向歐盟提出申請 GDPR 適足性認定的意願，「個人資料保護專案辦公



中央及地方政府參與「歐盟一般資料保護規則（GDPR）研討會」。

室」刻正盤點 GDPR 與我國個資保護法制的差異，撰擬我國個人資料保護整體架構的自我評估報告，盼盡速與歐方展開技術性對話，未來也將配合適足性諮商進程適時檢討我國個人資料保護法。

本次研討會邀請中央與地方政府同仁參與，首先由國發會介紹 GDPR 重點規範，包括 GDPR 背景與適用範圍、加重企業責任、強化當事人權利、跨境傳輸議題以及 GDPR 與我國個人資料保護法之比較分析等；另安排經濟部、交通部、金融監督管理委員會及國家通訊傳播委員會等相關部會分享因應 GDPR 的策略與作為，如調查 GDPR 對所轄產業的影響程度、調查產業資源



國發會陳主委於「歐盟一般資料保護規則（GDPR）研討會」開幕致詞。

需求、以及政府提供所轄產業的輔導及具體協助措施等；最後則透過專家學者的專題演講及產官學的綜合交流，分別從政府面及產業面討論因應 GDPR 的調適措施。

有鑑於我國個資法制架構係採分散式管理，由各中央目的事業主管機關與地方政府進行監督，對於因應 GDPR 施行對我國的衝擊及影響，實有賴中央與地方政府率先對 GDPR 加以掌握與瞭解，進而輔導與協助所轄產業，以全面落實個人資料的保護。國發會舉辦本次研討會，即是希望能夠透過對 GDPR 的介紹以及專家學者的分析與交流，加強公部門對 GDPR 的瞭解，以輔導與協助相關產業做好充足的準備。國發會後續亦將關注歐盟 GDPR 的發展動態，持續研議個人資料保護相關議題。🌀



「歐盟一般資料保護規則（GDPR）研討會」綜合座談。

GDPR 重點



擴大適用範圍



- 設立於歐盟境內之資料控管者 (data controller) 及受託處理者 (data-processor)；
- 設立於歐盟境外，但對歐盟境內之當事人提供商品或服務、或監控其行為之資料控管者及受託處理者 (§ 3)；此等企業原則應於歐盟設代表，受理相關事宜 (§ 27)。

GDPR 重點

強化個資保護

包括：書面委託歐盟境內代表、個資保護設計及預設、個資侵害事故通報與通知、個資保護影響評估、指定個資保護長、紀錄個資處理責任等。

擴大個資
定義

包括：透過網路IP、瀏覽紀錄產生之數位軌跡等。

加重企業
責任

強化當事
人權利

包括：更正權、刪除權(被遺忘權)、拒絕權、資料可攜權等。

提高罰則
金額

最高將處以2,000萬歐元或全球營業總額4%之行政罰。

GDPR 重點

限制個資跨境傳輸



資料跨境傳輸
原則禁止、例外允許

GDPR 規定個資傳輸至歐盟以外國家，應符合下列條件之一：

該國家取得適足性認定 (adequacy decision)

企業自主採行符合規範之適當保護措施

- 標準個資保護契約條款 (Standard Contractual Clauses)
- 拘束性企業規則 (Binding Corporate Rules)
- 行為守則 (Codes of Conduct)
- 取得認證 (Certification)

其他例外情形 (如個資當事人明確同意)

國發會作為



協調整合 GDPR 事宜



行政院於 107 年 5 月 24 日院會責成本會儘速成立「個人資料保護專案辦公室」，辦公室已於 107 年 7 月 4 日正式運作，二大工作重點為：

- 整合因應 GDPR 相關事宜，與向歐盟申請適足性認定工作。
- 配合檢討個人資料保護法，協調整合並加強各部會落實執行個資法之一致性。

近期工作重點：

- 為因應 GDPR 適足性認定相關工作，國發會已陸續召開多場跨部會會議、專家學者諮詢會議。
- 於 107 年 8 月 22 日召開以中央與地方政府為對象之 GDPR 研討會；另於 107 年 9 月辦理以企業為對象之北中南 3 場次 GDPR 宣導說明會。



本刊採清荷高環保道林紙
及環保大豆油墨印製

GPN: 2010300195
NT \$ 150元