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

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種次級法令中，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/EC[4] 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媺教授、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 GPDR。

【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媺教授、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。