專題報導

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

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 GDPR[4] 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	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）。 (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)	• last Revised and adopted on 5 April 2017 • WP242rev.01
2	資料保護長 (Data Protection Officers, DPOs)	• 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)	• last Revised and Adopted on 5 April 2017 • WP244rev.01
4	資料保護影響評估 (Data Protection Impact Assessment, DPIA)	• 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)	• 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)	• 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)	• Adopted on 3 October 2017 • WP 253
8	同意 (Consent under Regulation)	• last Revised and Adopted on 10 April 2018 • WP259rev.01
9	透明性 (Transparency)	• last Revised and Adopted on 11 April 2018 • WP260rev.01
10	驗證及驗證要件 (Certification and identifying certification criteria)	• Adopted on 25 May 2018 • Guidelines 1/2018
11	第49條特別規定 (derogations of Article 49)	• 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，事後的事故因應須更即時、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).