GDPR之國際傳輸

國發會法制協調中心

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，將牴觸 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。