我國面對歐盟GDPR個資保護浪潮之因應與挑戰：日本經驗之借鏡

⊙簡毓寧／中華經濟研究院第三（臺灣經濟）研究所　助研究員
⊙張馨云／普華商務法律事務所　律師
⊙王世明／中華經濟研究院第三（臺灣經濟）研究所　輔佐研究員

近年來隨著資通訊科技迅速發展，巨量數據廣泛應用於各項消費者行為分析、商品優化、交通管制及犯罪監控。個人資料之隱私權保護問題漸受國際關注，歐盟一般資料保護規則（GDPR）在此浪潮應蘊而生。其巨額罰款與嚴密的個資保護規範，堪稱國際當前最嚴格的個人資料保護法案。日本為亞洲第一個通過歐盟適足性認定的國家，故本文參酌日本對GDPR之相關因應措施，提出我國未來策略方向。

關鍵詞：一般資料保護規則、個資保護、日本經驗
Keywords: GDPR, Personal Data Protection, Japan Experience

數位經濟下的歐盟個資保護浪潮

隨著網路數位科技蓬勃發展，數據保存與傳輸過程的隱私權及使用權問題逐漸受到關注。網路媒體的消費者常為獲得某些優惠或娛樂服務，願意將個人部分資訊釋出。然而這些個人數據往往在當事人不自覺的情況下，受到額外的利用及分享。為因應雲端數據科技的迅速發展，同時兼顧消費者個人資料保護，經濟合作暨發展組織（Organization for Economic Co-operation and Development, OECD）積極倡議歐盟各國推動個人資料保護法規及發布應用個人資料的遵循原則。對此，歐盟遵循OECD原則框架，遂於1995年頒布「個人資料保護指令」（Data Protection Directive），2016年通過歐盟一般資料保護規則（General Data Protection Regulation, GDPR），並於2018年5月25日起全面實施新版個人資料保護規則。

GDPR規範內容主要有兩點，第一為擴大個人資料保護範圍，針對具有機敏性之個人資料，讓個資當事人得以保有個人資料的

修正、補充、刪除、暫時停止、限制、確認及拒絕應用範圍等權利；而資料可攜權之規定，則保障個資當事人得要求將其個人資料自由傳輸於不同控管者之權利；第二為加重風險管理機制及洩密罰則，GDPR規範個資控管者須於機構內設立個資保護官（Data Protection Officer, DPO），並針對所管控的個人資料進行個資風險分析（Data Protection Risk Assessment, DPRA），建立個資保護衝擊評估報告（Data Protection Impact Assessment, DPIA），以確實掌握當前個人資料處理活動對個資當事人的個資保護是否存在風險，研擬因應措施，詳實記錄及持續監控，並於個資外洩時即時通報以降低損害。而GDPR對於發生個資侵害事件時，也祭出高額罰款，依情節輕重最高處以2,000萬歐元或全球總營業額4%之罰款，以達警惕之效。

GDPR的適用範圍，以「存活的自然人」為其實體保護對象，並以「屬地主義」為其適用範圍。對於非歐盟國家而言，其適用範圍將涵蓋以下情境：（1）外國企業或機構在「歐盟境內」有營運據點；（2）外國企業或機構於蒐集個資的當下，其個資當事人正位於「歐盟境內」；（3）向「歐盟境內」之個資當事人販售商品或提供服務；（4）利用網路或穿戴式裝置等智慧科技，向「歐盟境內」的個人進行資料蒐集及監測等。前述可知，當外國企業或機構進行跨境個資傳輸，個資當事人是否位於「歐盟境內」為適用與否的關鍵，故若能取得「歐盟適足性認定」，將可在合法的途徑下任意與歐盟會員國進行個資跨境傳輸，消除觸法的疑慮。

日本面對GDPR之因應措施與策略

日本屬於數位科技高度應用且企業全球化程度高的國家，透過數位資訊、網路傳輸與雲端資料處理系統的迅速發展，建構出萬物聯網的雲端智慧生活空間。而歐盟GDPR跨境個資傳輸規定，直接衝擊日本企業與其他國家企業間可能具有的個資共有、移轉的情況；進而如何通過「歐盟適足性認定」為其積極推動的目標。對此，日本政府自2013年起陸續修正其個資保護法，並於2018年頒布「歐盟適足性認定之個人資料保護法相關補充規定」，使其符合國際規範，於2019年1月通過歐盟適足性認可，成為亞洲第一個取得適足性認定之國家。以下就日本個資保護制度及因應適足性認定而修正之法規內容，說明如下：

一、日本個資保護制度

日本個資保護法的設立始於2003年，並於2013年進行大幅度的法規修正，對於個資保護態度採行有效管理與謹慎利用的衡平策略。一方面聚焦於大數據的管理與應用；另一方面則致力於建構不侵害個人隱私的大數據分析環境，以利整體社會的發展。

其修法重點有五，第一，釐清現行法規的灰色地帶。隨著資通訊科技的快速推進，浮現新興數位科技應用模式，也創造出多元的電子數據蒐集與傳輸態樣。現行法規是否能有效地涵蓋，其灰色地帶尚待進一步釐清，故重新定義個資保護的範圍為此階段修法的第一要務。惟有建立完善的監督管理機制，方可讓民眾安心同意個資的有效利用。

第二，導入促進個資活用與利用機制。在日本舊有的個資法架構裡，個資提供第三方使用需經過當事人同意，惟此保護機制恐不利於巨量個資數據的正當利用。因此需積極規畫如何於不侵害個人隱私權利的前提下，透過提高資料去識別化程度，來達到有效利用之目的。第三，深化民間自主監督機制。鑒於剛性法律命令可能無法完整涵蓋個資保護範圍，將輔以民間自主監督機制以彌補現行法規不足之處。第四，建立專責機構。為確保個資保護機制之落實，於政府部門建立專責機構。第五，將現行法規與國際個資規範接軌。考量日本企業在全球化的趨勢下，勢將面臨個人資料的跨境傳輸與資料共享問題，故參考國際個資保護規範，將現行個資法規範內容與國際接軌，建立具國際信賴基礎的制度。

整體而言，觀察日本的個資保護法規修正方向不難發現，2013年的修正內容，已漸漸向歐盟GDPR規範靠攏。

二、日本適因應足性認定之法規修正

日本是否應爭取歐盟GDPR適足性認定之問題，其國內的因應態度有所不同。部分學者提出呼籲，指出儘管日本個資法未如GDPR嚴謹，然對於取得適足性之認定，應謹慎考量各國制度差異性，而非爭取歐盟適足性認定為單一目的。惟日本政府基於國家有權責整合國際制度，建構更完善的個人資料保護機制，因而選擇取得歐盟之適足性認定，並為達此目的，遂將現有制度增訂補充法規。有關日本為取得歐盟GDPR適足性認定而在制度上所訂定的補充規範，整理如下：

（一）修正敏感性個資之定義範圍：由於日本個資法尚未將GDPR所規範的「性生活」、「性向」及「工會組織」等個人資訊納入敏感性個資定義範圍。因此，透過此次修法將其增列；

（二）放寬保有個人資料之期限限制：日本個資法所謂保有個人資料，是指當個資管控者保有個人資料超過六個月的時間，其所保有之個資將受到日本個資法的保護。且個資持有者將有權限要求個資管控者，將其個資提供閱覽、訂正、追加、刪除、停止利用、停止提供給第三者。惟GDPR對於個人資料保護並無六個月的規定，因此基於歐盟之適足性認定而取得之個人資料，無論其保有的時間長短，皆適用個資法之相關規定；

（三）強化歐盟民眾個資利用目的之限制：加強日本業者蒐集來自歐盟境內民眾個人資料之「釐清」、「確認」、「紀錄」義務，並限定該資料的利用目的。除非再次取得當事人同意，否則不可做其他利用；

（四）傳輸個資予外國第三人之限制：對照於GDPR適足性規定，當日本資料控管者取得歐盟境內民眾個資後，若欲將其資料再提供予其他國家業者時，除該國需同樣符合個人資料輸出國的資格要求外，也需事前取得當事人同意；

（五）將去識別化後的歐盟個資納入匿名加工資料之規範範圍：對於接收來自歐盟的個人資料，經去識別化與不可復原之處理後，該資料視為匿名加工資料。日本政府此項補充法規之目的在於，許可對來自歐盟境內個人資

料進行匿名化處理，以利後續使用。

結語：日本因應策略之我國借鏡

透過日本的因應策略我們不難發現，其因應方針主要聚焦在處理跨國個資傳輸之問題，並以取得「歐盟適足性認定」為主要手段。為此目的，日本政府積極比對日本法與GDPR規範之落差，並透過頒布適當的補充法規，以通過適足性認定。

目前我國政府為因應歐盟GDPR的施行，國發會積極擬定因應措施，經法務部初步盤點，我國個資法與歐盟GDPR相比，臺灣在個資保護程度主要有兩大差異。一據行政院國家發展委員會所公布的資料指出，歐盟對於跨境傳輸採「原則禁止，例外允許」，臺灣則採「原則允許，例外禁止」。針對此一疑義，歐盟提出幾個允許跨境傳輸個資至歐盟境外國家的方案，符合以下三點的其中一項，即可允許跨境傳輸：包括該國家是否取得歐盟的適足性認定、企業組織是否自主實施符合GDPR規範之適當保護措施，以及其他例外情形等。換言之，適足性認定的取得，可為解決現行制度差異之途徑，以符合歐盟規範。

二為歐盟對於個資認定範圍較我國寬，法規亦更加嚴謹。惟依歐盟適足性認定之評估標準，其隱私保護制度需與歐盟保護程度相當，故檢視我國與之法規的落差實有其必要性。有關我國個資保護法規及GDPR的差異分析，大致可歸納以下三點，第一，領土適用範圍。無論是GDPR或日本個資法，皆將外國企業處理其境內民眾個資，納入個資保護的範疇。但因我國個資保護以境內企業所進行的個資處理為主，尚未針對外國企業或機構對於我國境內民眾之個資處理，建立保護機制；第二，個資當事人權利。我國賦予個資當事人權利相較於GDPR涵蓋範圍較小，較大差異處在於資料可攜權及被遺忘權兩項。在個資可攜權部分，目前對於個人資料於不同機構間之自由傳輸轉換尚有諸多限制；而被遺忘權部分，此點與我國現行醫療法對於個案病例資料之保存年限規定，有所牴觸；第三，個資管控之風險評估機制。GDPR規範機構（或企業）應設立個資保護人，並適時進行個資保護衝擊評估。惟此部分我國僅規定針對個資遭違法取得、不當修改、毀損、滅失或洩漏等保存不當行為，應採取技術上及組織上之措施，尚未針對個資保護及個資保護衝擊評估制定相關規定。

綜整前述，可發現我國個資法規、歐盟GDPR及日本個資法之規範範疇差異。儘管我國個資法已訂定諸多嚴謹規範，但對於通過歐盟GDPR所提出的設立獨立個資保護人、建立個資保護衝擊評估機制、擴大個資當事人權利範疇等，尚未建立具體細部的推動方針或修法建議。另值得注意的是，在日本的因應調整措施中，有關傳輸個資予外國第三人之限制，以及將去識別化後的歐盟個資納入匿名加工資料之規範範圍，是目前較少受到討論的項目。由於日本透過去識別化方式，擴充了歐盟境內民眾個資的合法利用範圍。本文建議未來政府亦可參酌日本經驗，評估其可行性及適用性，以利我國資料數據之應用與發展。