2018 年歐盟通用資料保護規則(GDPR)座談會

會議紀錄

一、 時間：107 年 4 月 11 日(星期三)下午 5 時 30 分

二、 地點：經濟部第一會議室

三、 主持人：王次長美花　　記錄：國合處暨資策會

四、 出列席單位及人員：(詳如簽名冊)

五、 主席致詞：略

六、 報告事項：略

七、 討論事項：

(一) 歐盟通用資料保護規則(EU General Data Protection Regulation，GDPR)影響企業範圍

GDPR 係史上最嚴格的歐盟個資保護規定，即將於本(107)年 5 月 25 日正式實施，適用於新興科技業人工智慧(Artificial Intelligence)、大數據(Big Data)、雲端(Cloud)、物聯網(Internet of Things)、金融科技(Fintech)、電子商務、資訊、電腦、網通、晶圓及薄膜電晶體液晶顯示器(Thin Film Transistor Liquid Crystal Display)等企業。

(二) GDPR 對於我國產業衝擊分析

在企業對消費者間衝擊較大者，包括使用大數據分析與雲端服務企業、進行跨境資料、處理、利用或分析歐盟消費者資料企業及處理、利用或分析歐盟特種個資企業；企業對企業間衝擊較小者，包括使用一般電子處理企業、於歐盟當地處理資料企業、僅有歐盟員工資料企

業及僅處理基本個資企業。

(三) GDPR 產業遵循重點

1.歐盟個資法域外效力：個資控制者或處理者在歐盟境內，不論資料處理是否發生於歐盟境內，若非設立於歐盟境內之資料控制者或處理者，對歐盟境內個資當事人提供商品、服務或對行為進行監控，亦適用之。

2.強化當事人權利：對當事人資料之蒐集及處理應符合透明化原則並取得明確有效同意，個資主體擁有被遺忘權(刪除)、向主管機關申訴、拒絕自動化決策及剖析權(Profiling)、近用權、可攜權、限制處理權等權利。

3.安全評估、設計及通報：須執行資料影響評估，並將設計著手保護隱私(Privacy by Design)、預先設定好的隱私權模式(Privacy by Default) 之資料保護原則內化為規則與措施，包含最小化、擬匿名化、透明化，確保系統及服務之保密完整可用性(Confidentiality, Integrity and Availability, CIA)，個資侵害事故發生後，於 72 小時內通報主管機關。

4.指派資料保護官(Data Protection Officer, DPO)與責任：核心業務涉及到對歐盟居民的資料處理，大型企業必須設立資料保護官，並有效依法履行職責。

5.避免鉅額罰責：非法處理、無故拒絕停止處理個資請求、個資資料外洩後未及時通知監管機構、未設立資料保護官，違法向第三國傳輸個資…等，最高將被處以 2,000 萬歐元或全球營業總額 4%的罰款。

(四) GDPR 遵循/認可的驗證單位

1.公認行為準則(Code of conduct, CoC)：根據 GDPR 第 40 條及 41 條規定，由產業協會或團體起草該產業遵循 GDPR 之行為準則，經歐盟監管機構核可，由歐盟資料保護委員會(EDPB)公告，並委由特定監督機構進行監督，惟目前無任何已公告通過 CoC，部分準則申

請中如 CSA GDPR CoC、CISPE、IIOC 等。

2.驗證/印章或標章：根據 GDPR 第 42 條及 43 條規定，國際驗證標準進行申請，運用認證機構/驗證公司之認驗證制度(ISO 17021/17025)，稽核管理有效性後核發證書。該驗證制度需經歐盟監管機構核可，由產業協會或團體起草該產業遵循 GDPR 之行為準則，經歐盟監管機構核可，由歐盟資料保護委員會(EDPB)公告，惟目前無任何已公告通過驗證標準/標章，部分標準/標章申請中如 CSA GDPR CoC、CISPE、IIOC 等。

(五) 企業因應 GDPR 優先行動方案之建議

1.規劃當事人權利行使管道及方式：針對GDPR要求之當事人權利如閱覽、近用權、申訴、拒絕自動化分析、資料剖析、更正、被遺忘權、撤回權等，規劃行使方式及管道，並需與資訊系統結合。

2.重新定義個資及資料流清：參照GDPR及其他區域性隱私資訊交換規範，除了新清查及定義個資欄位、數量、流向之外，進出入資料流均須重新鑑別法令遵循性，確認資料當事人是否屬於GDPR涵蓋範圍，並確認安全維護妥適性。

3.個資法遵要求與內控管理整合：個資法遵部門須根據歐盟法令與歐盟法院的判決，作出法律專業判斷，並配合可能的主管機關監督及查核，將個資保護措施納入，指派資料保護官及釐訂法律責任、分工，並納入管理循環。

4.資料安全維護義務強化：定義資料處理量、機敏資料保存量、規劃加密強度、去識別化、擬匿名化等安全維護措施標準，並隨業務成長持續監督改善。

5.強化隱私衝擊分析維度：隱私衝擊分析為強制要求，應考量DPbD&D (Data Protection by Design and by Default)系統設計，包含個資處理程式的相關紀錄及處理的軌跡。

6.強化個資盤點及作業流程盤點：個資盤點作業需重新進行，清查個資控制者、處理者及協力廠商，完整勾勒個資流向、個資儲存位置、負責單位及所在/國家。

(六) 我國銀行業、電信業及資安產業對於 GDPR 因應措施

1.銀行業：在歐洲設立據點的與會銀行代表表示，將配合 GDPR 規範設置資料保護官及資料保護單位，刻正進行銀行客戶資料差異分析、強化個資盤點，針對企業客戶備妥新的資料處理合約，其中包含 2010 年版個資保護條款契約(Standard Contractual Clauses, SCC)，因 GDPR 是屬地或屬人主義，4 大會計師事務所說法不一，尚需瞭解個別國家因應作法。

2.電信業：在歐州設立據點的與會電信業者詢問，業務涉及跨境傳輸服務，是否間接適用 GDPR 規範。與會 KPMG 代表回應，傳輸資料倘有蒐集歐盟人資料 device 及 IPO，依據 GDPR 第 42 條及 43 條規定，需取得國際驗證。

3.資安產業：資安業者表示，大多數之資安軟體皆設計蒐集大量訊息並分析，爰亟待瞭解 GDPR 所規範之訊息內容為何，以避免違反規定。與會 KPMG 代表說明，若是蒐集機型用於分析與統計故障模式，應不受 GDPR 規範，但若蒐集設備序號(可辨識相關人員)，則須受 GDPR 規範。建議在產品設計時即將此類要求納入考量，即以隱私為核心(DPbD&D)之精神設計。相關蒐集行為軌跡等資安設備與平台，依據其特性，會適用 GDPR 不同的要求，例如：資安設備的主要重點在於隱私敏感資訊的防護；分析平台則還要考量資料處理者應遵守的規範與資料控制者要求。

八、 臨時動議：無

九、 散會：晚間 8 時 20 分