臺灣證券交易所108年度研究報告提要表			填表人：董漢忠 填表日期：108年12月20日
研究項目	歐盟個資法(GDPR)帶來的省思－ 如何將個資保護精神整合入網站設計原理之探討		
研究單位及人員	資訊服務部 董漢忠	研究時間	自108年1月1日 至108年12月20日

報告內容提要

一、研究重點內容

本研究報告之研究動機為GDPR於2016年通過並於2018年實施，世界各國均可能受GDPR影響，開始重新檢討國內個資相關法令。本研究透過瞭解GDPR的發展過程，蒐集美、日、韓及我國政府的因應作為及近年度隱私權相關的案例，希望能對網站的設計提供建議以茲因應；網站設計如何強化以維護個資當事人權益，並在會員制或實名登記的網站，讓用戶資料得到更加完善的保護。

GDPR存在的目的，係為促使個人資料以合理及正當手段取得，並提升個資當事人權利與強化各國政府個資專責機關權限。GDPR之跨境傳輸原則為「原則禁止、例外允許」，美國及日本均與歐盟以新的協議或適足性認定完成因應；韓國與我國仍在適足性協商階段，兩國均卡在無獨立且具有執行權的個資監管機關故尚未通過適足性協商，企業仍須自行採取符合規範的適當保護措施方能執行跨境傳輸。

GDPR與我國個人資料保護法相比，主要差異為：

（一）**個資定義**：我國個資法，規範個資包含任何可識別自然人的資料，包含直接與間接資料；GDPR**則明確定義包含數位資料如IP、Cookie與GPS等在內**，並擴張間接資料的定義。

（二）**蒐集之合法前提**：我國個資法規定須依法告知目的、方式、內容欄位、利用方式及範圍、當事人權利，並取得同意；GDPR規範應提供的當事人權利中，定義更明確的**「被遺忘權」、限制處理，以可拒絕自動化分析及資料可攜權**；告知的內容型式應白話易讀，確保對當事人而言公平與透明。

（三）**組織內的準備**：我國個資法規定公務機關及企業必須配置管理人員及資源，設立管理機制並實作適當資料保護措施；GDPR規範蒐集前應進行**隱私衝擊評估**（DPIA）等程序，且如組織之核心活動為定期且系統性地大規模使用資料當事人者，應設立**資料保護長**（DPO）。

（四）**機器自動處理、分析與判斷**：我國個資法無相關規範；GDPR規範須事前評估，尤其是大規模的自動處理，不僅應**明確通知當事人，讓其可行使拒絕權、不被分析**、可要求刪除分析衍生的隱私資料，並且**須提供人為干預或救濟機制**。

（五）**事件通報**：我國個資法僅規定須於查明後以適當方式通知當事人；GDPR**規定要在72小時內通知主管機關，且必要時通知所有當事人**。

本研究報告剖析了蘋果、微軟及趨勢科技之因應GDPR做法，並運用「**資料保護設計與預設**(Data Protection by Design and by Default)」**之機密性、完整性、可用性、不可連結性、透明性以及可介入性**等6個特性，連同**最小化、隔離、抽象化、隱藏、通知、控制、執行、展示等8項指引措施**，做為建置抽獎活動網站及會員制網站之參考，使用戶資料的外洩機率降到最低並使外洩時傷害可以降到最低。

二、結論與建議事項

(一) 就GDPR與我國個資法差異，法律遵循面之因應措施：

1. **重新檢視各網站隱私權保護政策**：調整隱私權聲明及IP、Cookie等數位資料應用的範圍。
2. **個人資料保護相關輔助工具之設置**：以工具彙整個人資料散布情況及保存期限。
3. **評估個人資料保留時效與強化數位稽證之效力**：評估保存期限並自動化刪除；透過日誌軟體長期的蒐集彙整數位稽證。

(二) 就GDPR與我國個資法差異，程式開發及系統管理面之因應措施：

1. **重新檢視各網站設計是否合乎隱私工程原則**：就最小化原則評估，並檢視是否提供個資可攜權及拒絕被自動化分析權。
2. **研擬將隱私工程六大特性、八項指引納入系統開發準則內**：將尊重隱私的開發精神內化在設計理念內。
3. **強化資訊安全韌性、研究最新資安技術**：適時評估導入最新技術以維護個人資料安全。

將隱私工程技術納入網站設計原則中，透過合理及正當手段，獲得使用者個人基本資料，並提供個資當事人該有的權利，創建出更加「可信賴」的網站，讓使用者更放心的交付其個人資料。**本公司可在原本《個人資料保護法》的基礎上，因應GDPR增設規範項目進行網站設計調整，可以大幅降低必須從頭因應歐盟GDPR的高門檻。**