



經濟部因應 GDPR 施行 之策略與作法

經濟部



壹

前言

貳

經濟部因應 GDPR 施行之策略

參

經濟部因應 GDPR 施行之作法

- 歐盟於 2016 年通過 GDPR，2018 年 5 月 25 日正式施行，主管機關對違法者最高可處 **2000 萬歐元或年度全球營業總額 4 % (二者取其高者)**。
- 歐盟 GDPR 之適用範圍，包括 **歐盟境內之企業與未在歐盟境內之企業，但對歐盟境內之居民提供商品或服務或監控歐盟居民在歐盟境內之行為，而有蒐集處理與利用個人資料者**，本部所管產業部分有受到影響，如：

- ✓ 因雲端服務、APP 服務等 **網路應用服務或電子商務**，而有大量蒐集、處理或利用歐洲境內人民之個人資料
- ✓ **於歐盟境內設立代工廠、子公司、分公司、辦事室等據點者或大型品牌商** (對歐盟消費者銷售產品)

Distribution of Additional GDPR Compliance Budget
(Base: Falls Under GDPR, Will Spend More)



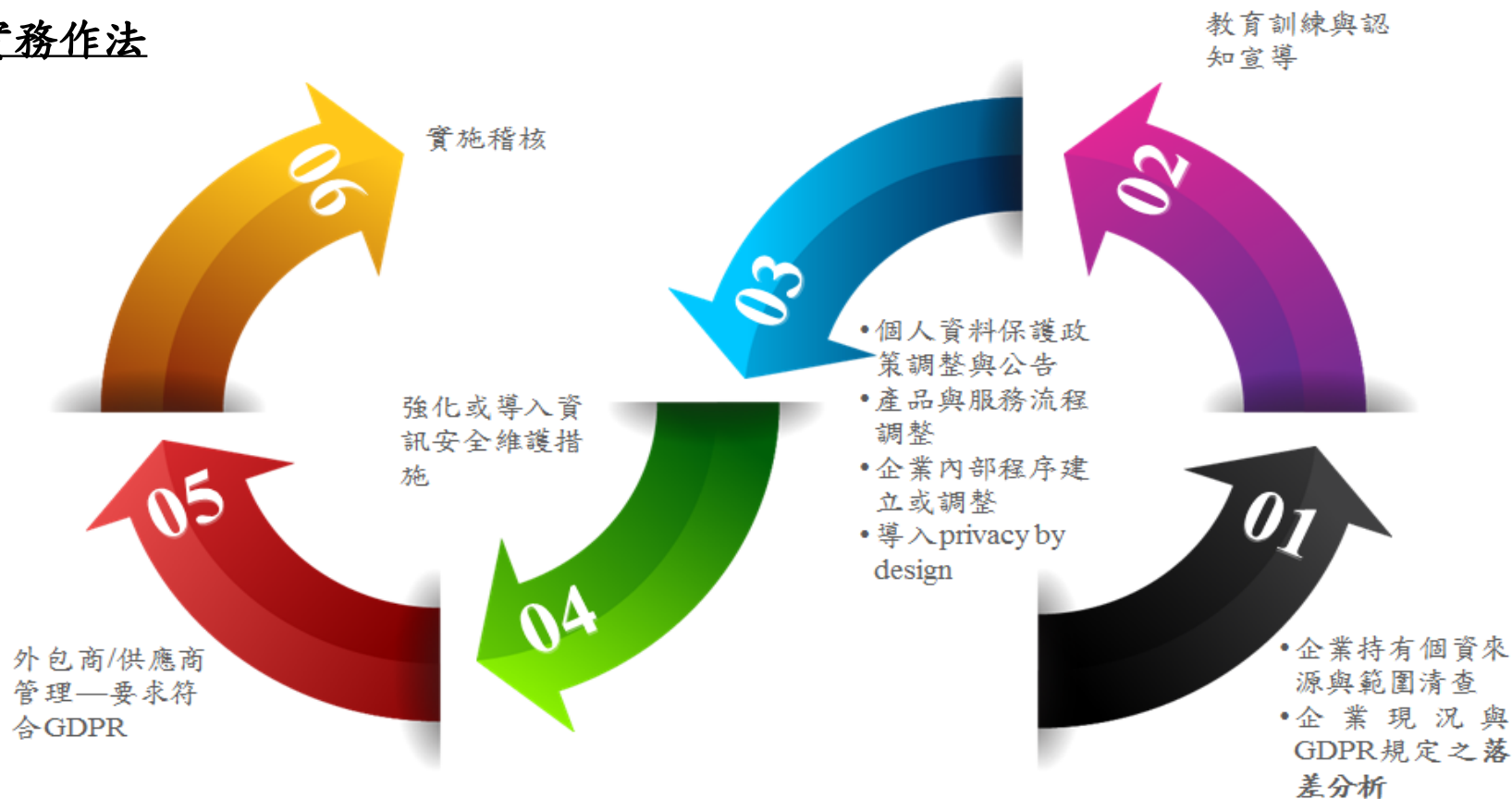
圖片來源：IAPP,2017

- 根據 IAPP 針對歐美適用 GDPR 之企業所為之調查，歐盟 GDPR 之施行為 **管理顧問、技術解決方案** (包括資安解決方案) 等帶來商機。

盤點產業因應 GDPR 之概況與最佳實務作法

透過座談會、業者訪問等方式，於**歐盟境內設立代工廠、子公司等據點者**或**大型品牌商**，為 GDPR 實施之直接衝擊對象。**已採取措施**因應 GDPR 之施行，如：**華碩、宏基**等大型品牌商。

實務作法





盤點產業因應 GDPR 之困難與需求事項

- 企業於因應 **GDPR 施行之過程**認有困難或困擾之處
 - GDPR 規定龐雜，部分規定抽象，不易判斷與掌握
 - 公司規模不大或資源有限，導致無法全面或充分因應
- 產業因應 **GDPR 施行過程中**希望受協助之事項
 - 法令與實作資訊之提供與諮詢
 - 顧問輔導與技術解決建議方案提供
 - 個資保護適足性認定
 - 驗證機制及其資訊之提供

協助產業因應 GDPR 施行之策略

- 降低資訊不充分，協助企業因應 GDPR 之施行
- 形成 GDPR 生態系，透過**資安服務團**協助產業因應 GDPR 與促進資安產業發展



01 降低資訊不充分，協助企業因應 GDPR 之施行

- 透過新興資安產業生態系推動計畫網站 (<https://www.acw.org.tw/>)，提供法規、實作、標準、顧問與解決方案提供者資訊、評估小工具等

[新鮮貨]技術專欄新增GDPR與雲端防護

2018-07-30

小編夏日推薦-6月與7月技術專欄新增3篇文章，歡迎大家點閱掌握最新產業趨勢!

- 6-26：[史上最嚴資料保護令5月上路，GDPR快易通與自我簡核表供您備戰不踩紅線](#) BY資策會
- 7-19：[Taiwan Information Security Solution Introduction / 台灣資安廠商介紹手冊](#) BY本計畫整
- 7-26：[雲端資安多層次防禦技術](#) BY工研院資通所

- 辦理座談會、說明會、交流會、分享會等，協助廠商了解 GDPR 及相關作法
 - 如：6/7、6/8 產業因應 GDPR 座談會、6/14 物聯網資安研討會、7/24 物聯網資安產業標準之廠商輔導及推廣說明、7/27 資安整合服務平台啟動大會等宣導
- 成立單一電話諮詢服務窗口，提供法規諮詢、資安顧問轉介服務

企業因應 GDPR 簡易自我評估表

填寫說明：

- 完成度 0-5，0 表示沒有規劃或程序，1 已有規劃但尚未進行，2 已進行 25%，3 已進行 50%，4 已進行 75%，5 表示 100%完成，請圈列。
- 於填寫本自我評估表前，請先行確認是否有下列情形，而有適用 GDPR 之情形
 - 於歐盟境內設有據點，包括但不限於公司或辦事處等任何形式。
 - 未於歐盟境內設立據點，但對歐盟境內之居民提供商品或服務，而有蒐集、處理或利用該等個人資料之情形。
 - 未於歐盟境內設立據點，但因追蹤或監控歐盟境內之居民的行為或活動，而有蒐集、處理或利用該等個人資料之情形。
- 另，提醒您如 貴公司為歐盟企業之供應商或外包商，而有為其蒐集、處理或利用個人資料之情形，仍應注意 GDPR 之規定。
- 本表僅為初步之自我評估，貴公司仍宜詳閱 GDPR 之規定，落實相關規定。如有需詢問之處，建議貴公司與本表之單一窗口聯絡，謝謝。

開始自我評估，GO!

項目	評分
1. 貴公司如未有於歐盟設立據點，是否有依歐盟 GDPR 之規定，於個人資料本人所屬國當地指定代表(representative)?	0 1 2 3 4 5

02

形成 GDPR 生態系，透過資安服務團協助產業 因應 GDPR 與促進資安產業發展

本頁詳如附件說明

- 建立**資安服務機構能量登錄**：於「技術服務機構服務能量登錄類別」新增「資安服務機構」，規劃**3項服務項目** 18分項 79小項分類國內資安產品及服務
- 成立**資安產業推動服務服務團**：提供資安供需雙方資訊分享及媒合平台
- 推動**資安檢測診斷服務**：遴選出關貿網路、漢昕科技、安華聯網，進行診斷服務並公開於**新興資安產業生態系推動計畫網站** (<https://www.acw.org.tw/>)，以協助產業找到適合的解決方案提供者

建立受檢測業者資格

建立檢測診斷流程

建立診斷驗收機制

優先順序

- 資安風險高低
- 個資數量多寡
- 影響社會民生程度
- 政策推動輔導產業

受測產業

- 資通訊製造業
- 雲端物聯網產業
- 金融服務產業
- 中小企業

風險評估

- 依造國際資安標準 ISO27000，檢視企業資安風險現況
- 逐步投入國際關鍵資安議題 (如 GDPR)

資安檢測

- 網路封包側錄分析
- 弱點掃描檢測
- 資訊設備組態基準檢測

顧問服務報告

- 資訊安全風險現況評估報告
- 資訊安全技術檢測報告
- 資訊安全風險控制建議報告



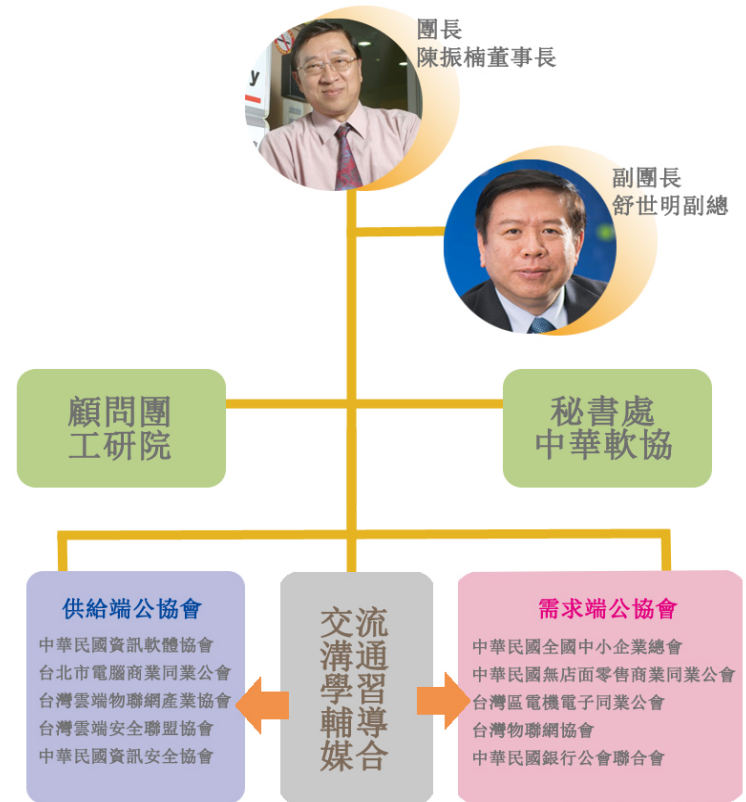
- 資安服務機構能量登錄：於「技術服務機構服務能量登錄類別」新增「資安服務機構」，規劃3項服務項目(18分項79小項分類)國內資安產品及服務：

- (1) 資訊安全管理顧問服務：包括資安管理系統、政策、程序的建立。
- (2) 資訊安全檢測服務：整體資安防護與治理，並提供解決方案。
- (3) 資訊安全服務、建置及產品服務：資安產品提供解決特定領域問題。

- 資安產業服務團

為從產業推動跨域資安，提升產業資安基礎防護能量，健全資安產業發展環境，**透過鏈結相關公協會，成立資安產業服務推動團**。資安產業服務團由中華資安董事長擔任團長、勤業眾信副總擔任副團長。其中邀請全國中小企業總會參與，以呼應全國各領域中小企業對資訊安全之需求。

透過服務團建立供需資訊分享(如GDPR、產業趨勢)與資安健檢服務，經由檢測診斷彙整之產業資安現況及改善建議，回饋各公協會提供其會員參考導入，達到擴散成果之效益。



- 關於資安能量登錄或資安產業服務團進，可洽：
中華民國資訊軟體協會鄭小姐 / (02)2553-3988 #387