有關歐盟個人資料保護規則(GDPR)施行對我國之影響及因應策略

一、 背景說明

隨著數位經濟科技發展與全球化影響，個人資料之保護日趨重要。歐盟為提升個人資料保護規範密度，並建立歐盟境內一體適用之管理規範，於 2016 年 5 月 24 日通過「個人資料保護規則」(General Data Protection Regulation, GDPR)，以取代歐盟 1995 年個人資料保護指令(Data Protection Directive)，並將自今(2018)年 5 月 25 日全面施行。GDPR 之施行，將提高企業管理個人資料之法遵成本，並適用於在歐盟境內設立據點或與歐盟業務往來之企業，已引起各國高度重視。

我國與歐盟間雙邊經貿往來一向密切,GDPR之施行，勢將廣泛影響我國在歐盟營運或對歐從事業務之企業。政府必需積極研議因應策略，以協助相關企業採行適當個人資料保護措施，並與歐盟展開對話，取得歐盟認可我國對個人資料保護具適足程度，以利企業與歐盟間進行個人資料跨境傳輸活動。

二、 GDPR 重要內容

(一)擴大適用範圍

設立於歐盟境內，涉及個人資料處理之控制者及受託者；非設立於歐盟境內，對於歐盟境內之個人資料當事人為：1.提供商品或服務；2.對歐盟境內的行為進行監控之資料控制者及受託者。

(二)對個人資料定義較廣

得直接或間接識別出特定當事人之資料類型，例如網路瀏覽器 Cookies、網路 IP 位址等皆屬之。

(三)明確有效同意

個人資料之取得必須由個人資料當事人自由提供、具體、知情及明確同意。

(四)擴充個人資料當事人權利

包括更正權及被遺忘權（刪除權）、資料可攜權、拒絕權（拒絕自動化分析）等。

(五)舉證責任

資料控制者應負符合 GDPR 規定之舉證責任。

(六)設計及預設之個人資料保護

應實施科技化且有組織的措施，將隱私保護納入程式設計，以確保處理程序符合 GDPR 要求之保護個人

資料當事人權利。

(七)書面委託歐盟境內代表

非設立於歐盟境內，但對於歐盟境內人民提供商品或服務或監控其行為者，除偶然性之處理或公務機關外,均應以書面委託歐盟境內之代理人作為代表，受理主管機關或個人資料當事人提出之要求。

(八)文件化紀錄責任

應負責維護資料處理活動之紀錄;員工人數低於 250 人之企業可除外,但經常性處理或係涉及特殊類型、犯罪個人資料者，仍適用之。

(九)個人資料外洩通報

發生個人資料外洩事件，應於知悉後 72 小時內通報當地個人資料主管機關；若對個人資料當事人之權益有重大危害之虞，亦應通知當事人。

(十)個人資料保護影響評估

個人資料處理可能造成個人資料當事人高度風險者，應於處理前執行個人資料保護影響評估，尤其是大規模的個人特質評估、處理特殊類型或犯罪個人資料、監控公共領域者。

（十一）指定個人資料保護長

涉及大規模監控個人資料當事人；或大規模處理特殊類型、犯罪個人資料者，應指定個人資料保護長。

（十二）個人資料跨境傳輸

歐盟採「原則禁止、例外允許」模式， 例外情形如取得適足性認定、企業自主採行符合規範之適當保護措施(例如：標準個人資料保護契約條款、有拘束力之企業守則、行為守則、取得特定認證等)或個人資料當事人明確同意，始得傳輸至歐盟境外。

（十三）提高罰則金額：

最高將處以 2000 萬歐元或全球營業總額 4 %之行政罰鍰。

三、 GDPR 對我國之影響

依 GDPR 規範內容分析，GDPR 對我國企業主要衝擊為在歐盟設立據點、對歐盟境內人民提供產品或服務、監測歐盟境內人民網路行為之業者。考量 GDPR 主要係從個人資料可能發生風險之角度，課予資料控制者及受託者不同程度之義務。因此，我國相關企業涉及大規模處理個人資料、大規模跨境傳輸、使用大數據分析或雲端

服務或在歐盟經濟活動規模較大者，其遵法成本亦將大幅提高。

另一方面，相關企業員工人數未達250人且營業活動係偶然性處理或不涉敏感性個人資料者，可免除維護資料處理活動紀錄之義務；另若無大規模監控個人資料當事人或無大規模處理敏感資料者，亦無須設置個人資料保護長。

至於有需求與歐盟進行跨境傳輸個人資料之相關企業，由於歐盟係採「原則禁止、例外允許」模式，因此在我國未取得歐盟認定為適足性保護之國家前，企業仍應依GDPR 規範，選擇採行標準契約條款、拘束力之企業守則、行為守則或取得認證等方式，進行個人資料傳輸。

為協助產業因應GDPR施行後可能造成之衝擊與影響，短期而言，政府除應提出GDPR之相關重點資料供業界參考運用，各中央目的事業主管機關則應就所轄產業規劃因應措施並提供輔導與諮詢協助；長期而言，政府應逐步推動與歐盟洽商有關跨境傳輸適足性認定事宜。

四、　因應策略與部會分工

（一）由國發會會同各部會辦理下列事宜，並公布於國發

會網站，以利外界參考運用：

1. 國發會負責編撰GDPR重要內容介紹與說明文件。
2. 法務部提供GDPR與我國個人資料保護法之比較與分析。
3. 經濟部、金管會、國家通訊傳播委員會、交通部等相關部會，提供業管產業有關企業因應GDPR之輔導與諮詢服務，並提供具體工作進度及辦理情形。

(二)由國發會主政，並會同外交部、法務部及個人資料保護相關中央目的事業主管機關，向歐盟申請適足性認定事宜。