

歐盟「一般資料保護規則」 (General Data Protection Regulation, GDPR) 簡介與因應

國家發展委員會

大綱



背景



GDPR 重點



跨境傳輸議題分析



GDPR 對我國企業影響

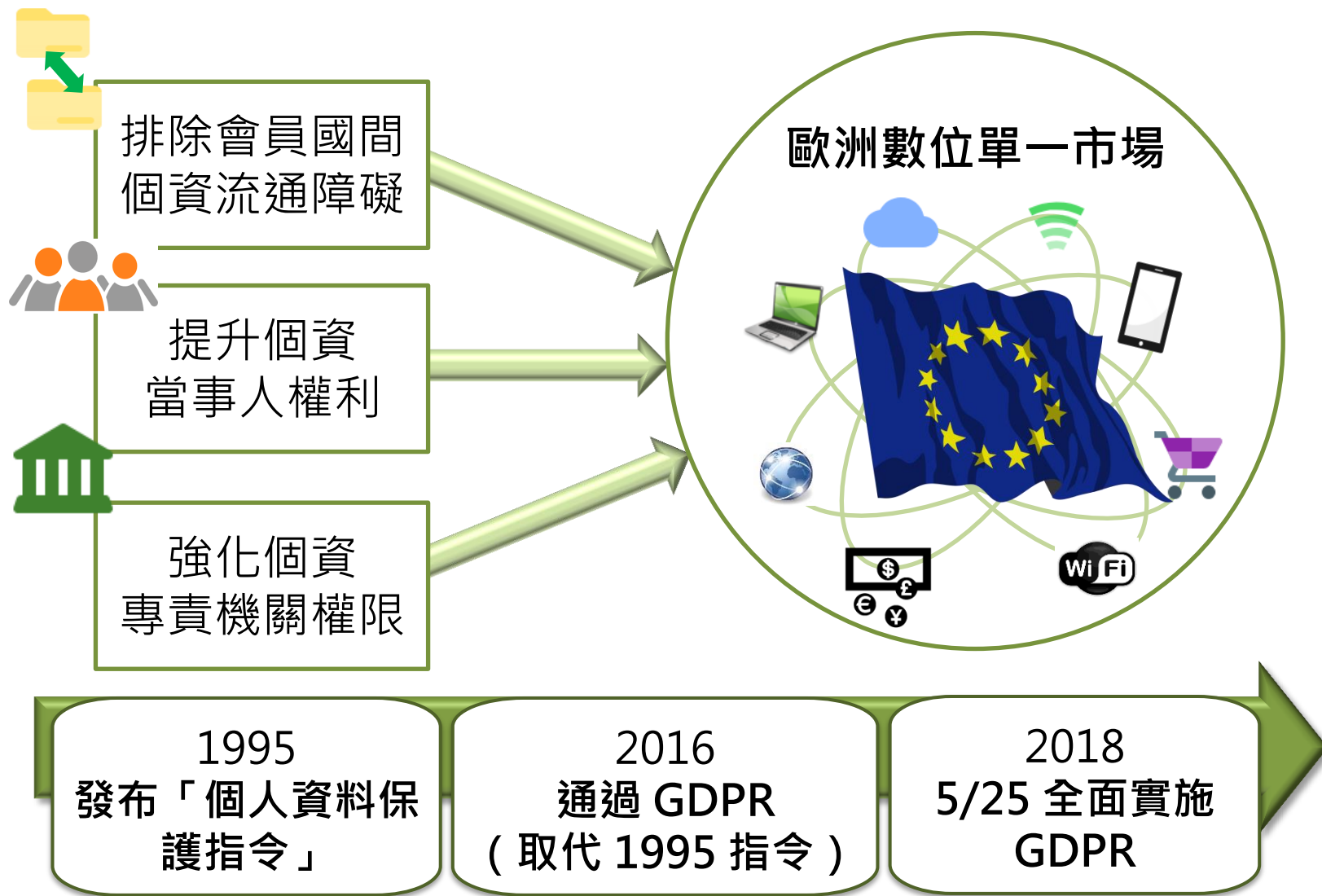


盤點法規



結語

背景



擴大適用範圍



- 設立於歐盟境內之個資處理控管者（ data controller ）及受託處理者（ data processor ）；
- 設立於歐盟境外，但對歐盟境內之當事人提供商品或服務、或監控其行為之資料控管者及受託處理者（ §3 ）；此等企業原則應於歐盟設代表，受理相關事宜（ §27 ）

擴大個資定義

一般個資



得以直接或間接方式識別當事人之任何資訊。

包括：透過網路 IP、瀏覽紀錄產生之數位軌跡並得追蹤識別特定當事人之身分。

特種個資



揭露人種、血統、政治意見、宗教、哲學信仰、工會身分、基因、生物特徵、健康相關、性生活與性傾向之資料。

明確當事人同意

不構成同意：

- 單純沉默。
- 預設選項為同意。
- 不為表示。



當事人自由提供、具體、知情及明確同意。

撤回：

同意之撤回應與給予同意一樣容易。

目的：

個人資料之處理具有多重目的者，應就全部目的取得同意。

加重企業責任

§83

最高將處以 2000 萬
歐元或全球營業總
額 4 % 之行政罰。

§24

在技術上及組織
上納入隱私保護
措施。

§33

應於知悉後 72 小時內
通報當地個資主管機
關必要時並應通知當
事人。

提高
罰則金額

個資保護
影響評估

個資保護
設計及預設

指定
個資保護長

個資侵害事故
通報與通知

文件紀錄
責任

§35

個資處理可能造成當
事人高度風險者，應
事前執行個資保護影
響評估。

§37-39

涉及大規模監控個資
當事人；或大規模處
理特殊類型、犯罪個
資者。

§30

員工 250 人以上企
業原則應保存維護相
關紀錄。



強化當事人權利



限制個資跨境傳輸



資料跨境傳輸—
原則禁止、例外允許

該國家 / 地區取得適足性認定
(adequacy decision) (§ 45)

企業自主採行符合規範之適當保護
措施 (§40、42、46、47) :

- 標準個資保護契約條款
(Standard Contractual
Clauses)
- 拘束性企業規則 (Binding
Corporate Rules)
- 行為守則 (Codes of Conduct)
- 取得認證 (Certification)

其他例外情形：
如個資當事人明確同意 (§49)

例外允許跨境傳輸

GDPR 規定個資傳輸至歐盟以外國家，應符合下列條件之一：

- 
- 該國家取得適足性認定（adequacy decision）
 - 企業自主採行符合規範之適當保護措施
 - 其他例外情形

適足性認定評估項目

評估	內容
整體考量	• 法制環境。 • 獨立監管機關。 • 簽訂國際協定或合約。
國家選擇	• 雙邊經貿關係。 • 資料傳輸量與頻率。 • 是否為該地區的隱私保護先進國。 • 政治關係。 • 隱私保護系統是否與歐盟保護程度相當。
認定程序	• 該國主動提出，雙方進行技術性對話。 • 歐盟內部獨立專家提出評估報告，並由歐盟執委會提案，送交歐洲資料保護委員會（EDPB）提出意見。 • 歐盟國家代表批准是否具適足性。

*目前歐盟執委會積極合作對象：日本、韓國、印度、拉丁美洲及歐洲鄰近國家等。另目前已有 12 國家 / 地區獲適足性認定。

自主採行適當保護措施

保護措施	內容
標準個資保護契約條款 (Standard Contractual Clauses)	適合採用之企業：經常性接收某一歐盟境內公司個資。
拘束性企業規則 (Binding Corporate Rules)	- 歐盟境內企業集團內或從事於共同經濟活動之企業集團間，移轉個資應遵守之保護政策。 - 適合採用之企業：母子公司跨國企業。
行為守則 (Codes of Conduct)	- 應考量對微型及中小型企業特定需求。 - 適合採用之企業：業務僅涉及特定業別。
取得特定認證 (Certification)	- 目前歐盟層級之認證尚未施行，歐盟會員國已各自有認證機制。 - 應考量對微型及中小型企業特定需求。 - 適合採用之企業：業務僅涉及特定業別。

其他例外情形

其他例外情形	內容
個資當事人明確同意	告知個資當事人可能之風險後，取得當事人明確同意移轉。
其他必要措施	例如： • 因執行契約所必要。 • 基於公共利益之重要原因。 • 於個資當事人無法為同意之表示，移轉對其有重要利益保護必要。

小結

- 從事跨境傳輸之企業，在我國尚未取得適足性認定前，應依 GDPR 規範，評估選擇採行標準個資保護契約條款（SCC）、拘束性企業規則（BCR）、行為守則（CoC）及認證（Certification）4 種國際傳輸方式，或符合其他例外情形。

影響程度



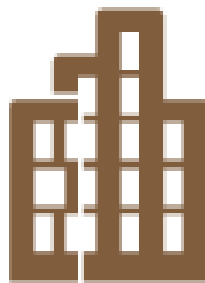
- 非設立於歐盟境內

- 偶然性處理歐盟個資

- 於歐盟境內處理個資

- 使用一般電子處理

- 在歐盟經濟活動規模較小



- 設立於歐盟境內。
- 非歐盟境內，但對歐盟人民提供商品或服務、監控其行為。

- 大規模處理歐盟個資

- 進行跨境傳輸

- 使用大數據分析或雲端服務

- 在歐盟經濟活動規模較大

GDPR 與我國個資法之比較

GDPR	個資法
歐盟境外企業對於歐盟境內當事人提供商品、服務或監控其於歐盟境內行為，該個資處理活動仍適用 GDPR。	規範對象 適用地域 我國公務及非公務機關於境外對我國人民個資之蒐集、處理及利用，亦適用我國個資法。
• 一般：得以直接或間接方式識別當事人之任何資訊，包括透過網路 IP、瀏覽紀錄產生之數位軌跡並得追蹤識別特定當事人之身分。 • 特種：揭露人種、血統、政治意見、宗教、哲學信仰、工會身分、基因、生物特徵、健康相關、性生活與性傾向之資料 • 刑事：前科與犯罪紀錄。	個資定義 • 一般：得以直接或間接方式識別個人之資料。 • 特種：病歷、醫療、基因、性生活、健康檢查及犯罪前科等。

GDPR 與我國個資法之比較

GDPR		個資法
應符合合法性、公平性及透明度、利用目的限制、資料最少蒐集、正確性、儲存限制、完整性與保密性等處理原則。	個資處理原則	應依誠實及信用方法，不得逾越特定目的之必要範圍，並應與蒐集之目的具正當合理關聯。
更正權、刪除權、 個資可攜權 、拒絕權。	當事人權利	請求製給複製本、更正權、刪除權、拒絕權。
原則禁止、例外允許。	跨境傳輸	原則允許、例外禁止。

GDPR 與我國個資法之比較

GDPR		個資法
至少 一個獨立公務機關 ，監督 GDPR 之適用。	監管機關	分散式管理制度 ，各中央目的事業主管機關執行檢查、糾正、裁罰權。
- 個資保護影響評估。 - 指定個資保護長。 - 文件紀錄。 - 知悉個資侵害事故 72 小時內通報與通知。 個資保護之設計及預設。	企業責任	- 個資風險評估。 - 配置管理人員。 - 使用紀錄及軌跡資料與證據保存。 - 事故通報及應變機制。 - 設備安全管理。

國發會協調整合 GDPR 事宜

行政院於 107 年 5 月 24 日院會責成本會儘速成立「個人資料保護專案辦公室」，辦公室已於 107 年 7 月 4 日正式運作，二大工作重點為：

- 整合因應 GDPR 相關事宜，與向歐盟申請適足性認定工作
- 配合檢討個人資料保護法，協調整合並加強各部會落實執行個資法之一致性

GDPR 相關網路資源

本會已於官網設置專區，適時更新 GDPR 相關資訊，包括：

- GDPR 簡介
- GDPR 導讀
- 法規翻譯（含 EDPB 採認文件之連結）
- GDPR 與我國個資法之比較分析

🏠 首頁 > 主要業務 > 法制協調 > 個人資料保護專案辦公室 > 歐盟一般資料保護規則專區

歐盟一般資料保護規則專區



隨著數位經濟科技發展與全球化影響，個人資料保護議題帶來許多新的挑戰，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「一般資料保護規則」(General Data Protection Regulation, GDPR)，以取代歐盟1995年個人資料保護指令(Data Protection Directive)，並自今(2018)年5月25日全面施行。

為因應GDPR施行後可能造成之衝擊與影響，本會已於今年4月間邀集各部會積極研議相關因應策略，為利各界瞭解GDPR相關重要資訊，爰建置本網頁，並提供GDPR簡介、翻譯資料、相關部會諮詢窗口以及GDPR與我國個人資料保護法之比較分析，相關資訊將隨時更新。

▶ 歐盟GDPR簡介

▶ 歐盟GDPR導讀

▶ 歐盟GDPR法規

▶ 歐盟GDPR與我國個人資料保護法之重點比較分析

▶ 歐盟GDPR之相關部會諮詢窗口

簡報結束