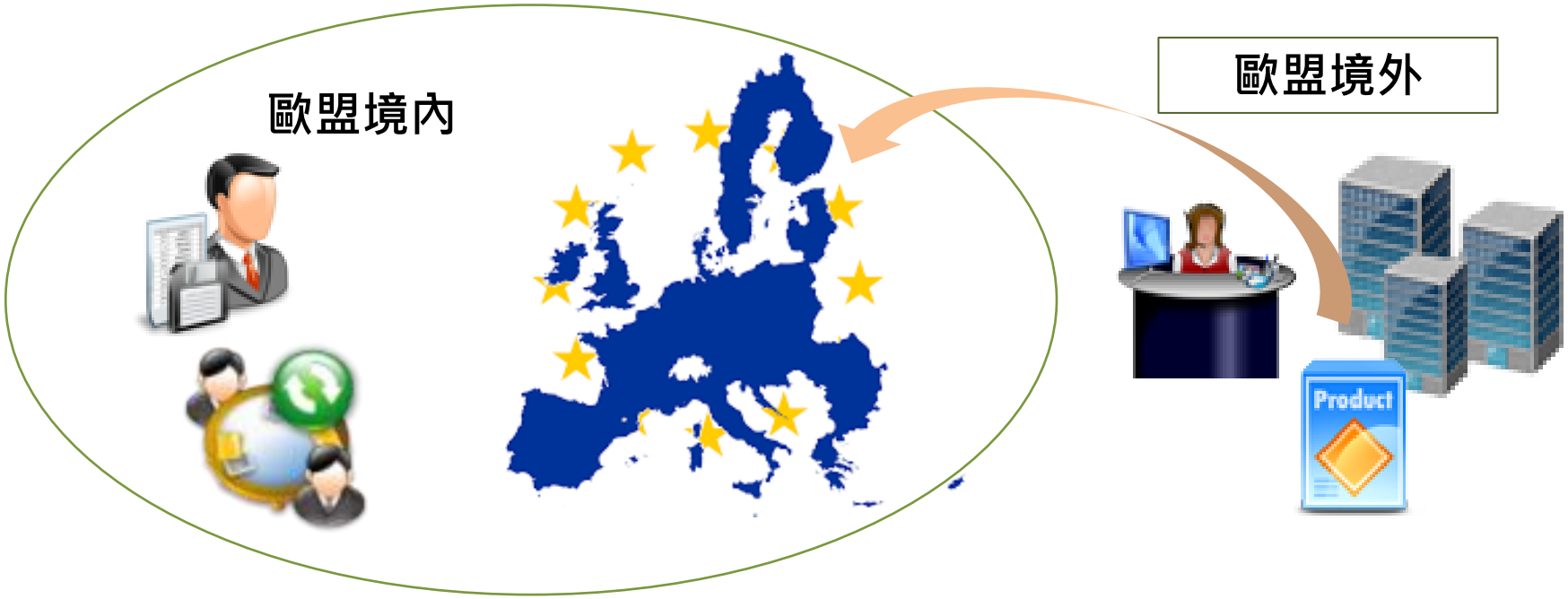
歐盟「一般資料保護規則」(GDPR)及因應措施

國家發展委員會
報告人：法制協調中心林主任志憲
107 年 7 月 13 日

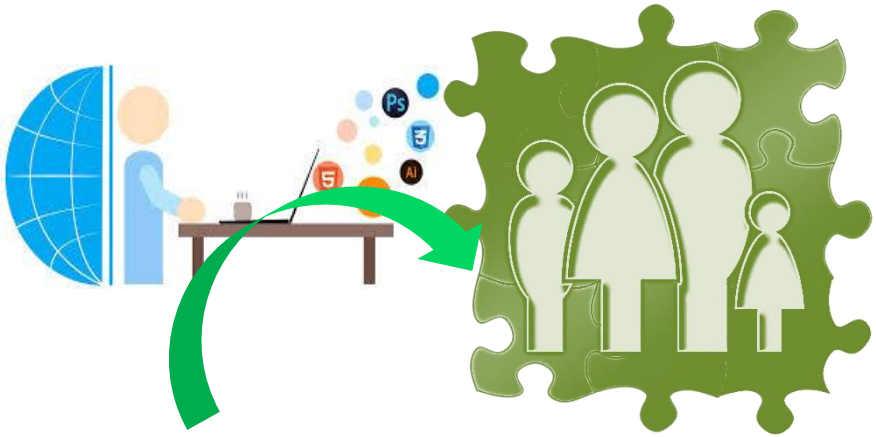
擴大適用範圍



- 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

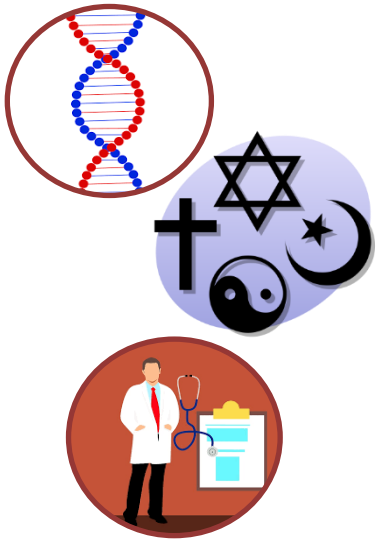
一般個資



得以直接或間接方式識別當事人之任何資訊。

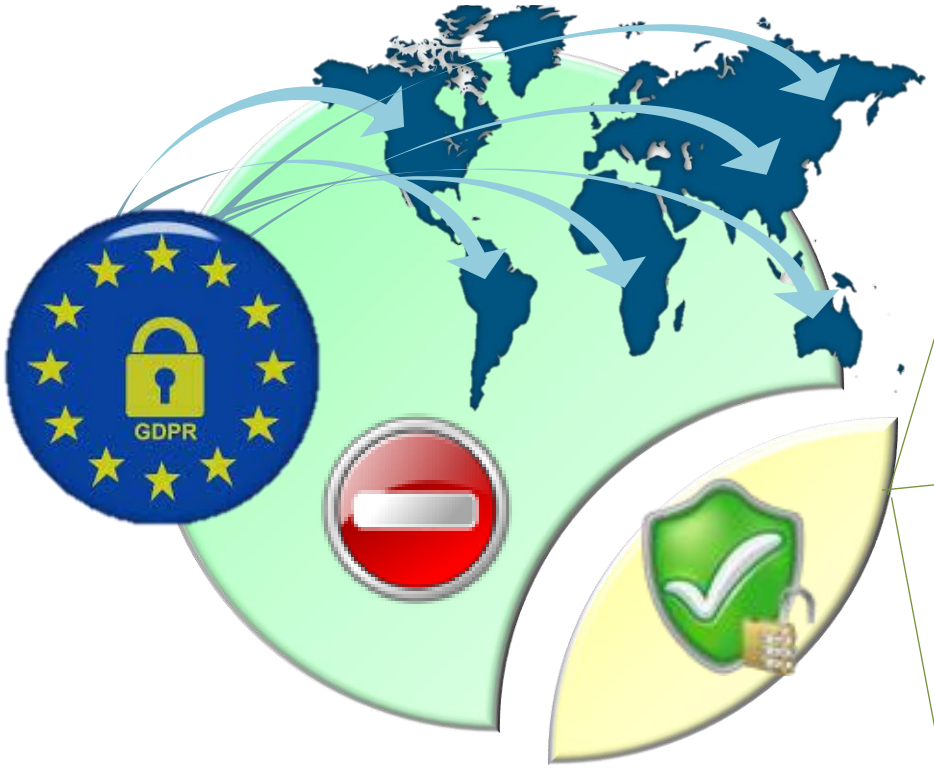
包括：透過網路 IP、瀏覽紀錄產生之數位軌跡並得追蹤識別特定當事人之身分。

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。

限制個資跨境傳輸



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）

資料跨境傳輸—
原則禁止、例外允許

盤點法規差異

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。

盤點法規差異

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。

盤點法規差異

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。

結語

因應 GDPR 之施行，本會已成立「個人資料保護專案辦公室」，並於 107 年 7 月 4 日正式掛牌運作。本辦公室主要任務為整合因應GDPR相關事宜，並負責向歐盟申請適足性認定，以及檢討我國個資法，強化各部會落實執行個資法之一致性。

簡報結束