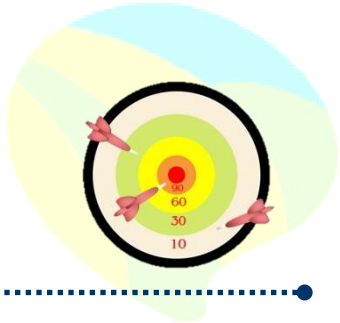
國家通訊傳播委員會
NATIONAL COMMUNICATIONS COMMISSION

跨境隱私保護最新趨勢剖析

財團法人資訊工業策進會
科技法律研究所

stli 科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

大綱



一 跨境隱私與個人資料保護

二 APEC跨境隱私保護規則體系（CBPRs）介紹

三 歐盟通用資料保護規則（ GDPR ）介紹

簡介：APEC CBPRs

◆APEC跨境隱私保護規則體系（APEC CBPRs）

➢亞洲太平洋經濟合作會（Asia-Pacific Economic Cooperation）下的「跨境隱私保護規則體系」（Cross Border Privacy Rules System, CBPRs）

➢係由APEC會員經濟體所共同參與，經尋求企業和社會各界的意見後制訂，以期建立消費者、企業和監督管理者對個人資料跨境流動之信任。

➢我國為APEC會員經濟體之一，目前積極爭取加入CBPRs

簡介：EU GDPR

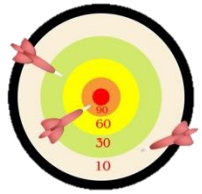
◆歐盟通用資料保護規則（EU General Data Protection Regulation , GDPR）

- 目的：為了統合歐盟各國隱私與個資保護標準，原本歐盟會員國間之個人資料保護相關法律缺乏統一架構
- 新科技所衍生之資通訊技術對隱私及個人資料之保護衍生出新的實務議題、法令衝擊與挑戰
  - ✓ 大數據（Big Data）
  - ✓ 物聯網（Internet of things, IoT）
  - ✓ 雲端計算（Cloud Computing）
- 於2018年5月25日正式施行
  - ✓ 2016年4月歐洲議會通過歐盟規則2016/679，自2016年5月24日起生效
- 1995年個人資料保護指令(EU Directive 95/46/EC: the Data Protection Directive)

大綱

一 跨境隱私與個人資料保護

二 APEC跨境隱私保護規則體系（CBPRs）介紹



三 歐盟通用資料保護規則(GDPR)介紹

APEC CBPRs 概述

1998 APEC電子商務行動藍圖計畫
（APEC Blueprint for Action on Electronic Commerce）隱私保護9項原則

2005 APEC隱私保護綱領
（APEC Privacy Framework）

2007 APEC開路者倡議實驗計畫
（APEC Data Privacy Pathfinder Projects）

2011- **跨境隱私保護規則體系（Cross Border Privacy Rules System, CBPRs）**

APEC CBPRs: 目的

◆ CBPRs：建立資料跨境傳輸共通原則

- **目的：協助APEC會員經濟體發展有效之個人資料隱私保護措施以及企業從事相關活動**

- **促進跨境資料自由流通**
  - ✓ 個人資料的跨境流動可能為潛在的貿易障礙
  - ✓ 為保護個人資料不被濫用，各國個資法規不一，跨境業者難以應付
  - ✓ 為協助APEC會員經濟體發展有效之個人資料隱私保護措施

- **會員經濟體：**目前美國、墨西哥、日本、加拿大、韓國、新加坡等已加入CBPRs。美國尤其大力提倡。

- 我國積極準備加入中

APEC CBPRs: 機構與運作

CPEA
執法機關管理者
CPEA
Administrators

聯合監督工作小組
Joint Oversight Panel
（JOP）

政府

隱私執法機關
Privacy Enforcement Authority (PEA)

- 確定經濟體內隱私保護法符合體系要求
- 違反隱私保護事件調查
- 促進經濟體間資訊分享、合作
- 隱私保護問題事件轉介
- 接受消費者提問、申訴

公正第三方

問責機構
Accountability Agent (AA)

- 審查、認可企業組織
- 接受消費者提問、申訴

民間

企業組織
Organization

- 提供隱私保護政策與準則
- 遵循政策與準則
- 接受消費者提問、申訴

APEC CBPRs: 已加入成員

經濟體	加入時間	執法機關（PEA）	問責機構（AA）
美國	2012年 7月	美國聯邦貿易委員會 （Federal Trade Commission, FTC）	TRUSTArc (原TRUSTe)
墨西哥	2013年 1月	墨西哥聯邦公共資料近用與資料保護機構 （Federal Institute of Access to Information and Data Protection）	
日本	2014年 4月	個人情報保護委員會 (Personal Information Protection Commission, PPC) (2015年修正個人情報保護法，統一執行監督機關)	日本情報經濟社會推進協會 （JIPDEC）
加拿大	2015年 4月	加拿大隱私委員 （Privacy Commissioner of Canada）	
韓國	2017年 6月	內政部、韓國通訊委員會 （Korea Communications Commission）	
新加坡	2018年 3月	新加坡通訊及新聞部 （Ministry of Communications and Information）	

APEC CBPRs: 問責機構

- 任務：就參與企業之隱私政策及做法進行認證，並確保其符合CBPRs之要求。
- 透過CBPRs，問責機構與企業、消費者及政府協同合作，確保跨境個人資料之傳輸，符合APEC隱私保護綱領所要求之標準，並解決所產生之任何爭議。
- 經CBPRs所認可之問責機構，除可利用CBPR問卷 及CBPR計畫要求條件評估企業或其他組織是否合規外，亦得使用自有之隱私認證計畫。

APEC CBPRs: 企業申請認可程序與條件

APEC CBPRs: 小結

1.促進貿易與隱私

2.增進跨境隱私執法合作

3.將第一線執法外放予AA，政府將可更專注於高衝擊、高風險隱私爭議

4.協助調查洩露隱私案件與執法

1.展現組織問責制

2.創造消費者信賴

3.統一組織隱私保護標準（尤其是跨國企業）

4.有效且彈性之自律或共同監管規範

5.隨著參與經濟體之增加，將可降低跨境法遵成本。

1.強化隱私保護

2.簡化投訴處理

3.增進消費者信賴

政府

企業

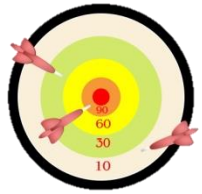
消費者

大綱

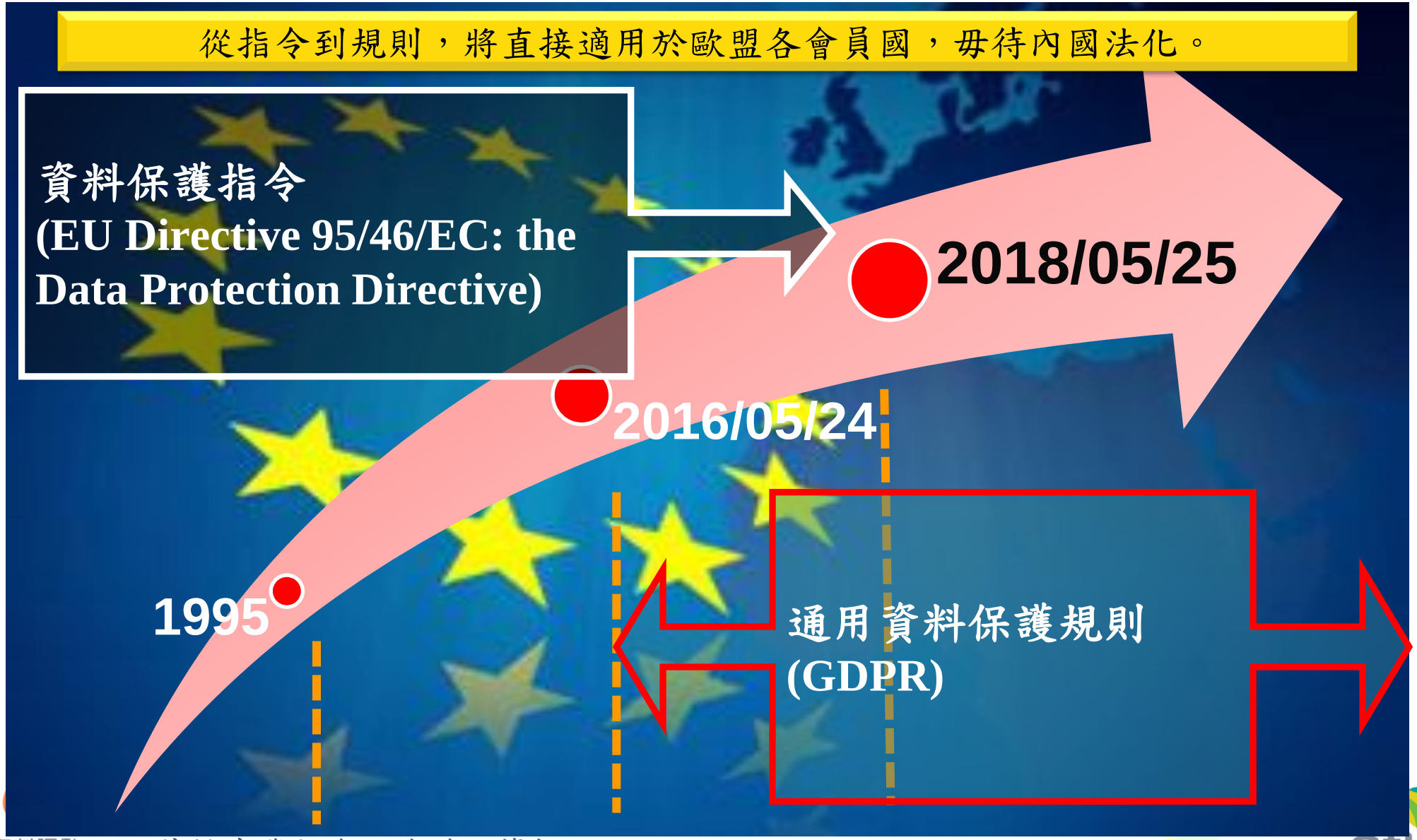
一 跨境隱私與個人資料保護

二 APEC跨境隱私保護規則體系（CBPRs）介紹

三 歐盟通用資料保護規則(GDPR)介紹



GDPR: 執法進程



GDPR: 六大原則

適法、公平、透明

應以合法、公平且透明的手段處理個人資料

目的限定

應以特定、明確且合法的目的蒐集個人資料，且不得以與目的不相容的方法進一步處理該個資

個資最小化

應對照處理個人資料之目的之必要性，以適當、且具關連性，並在最小限度內處理個人資料

正確性原則

個人資料必須要保持正確，並且於必要時確保其為最新的資料。不正確的個人資料，應採取各種合理的手段，確保確實且立即刪除或予以訂正

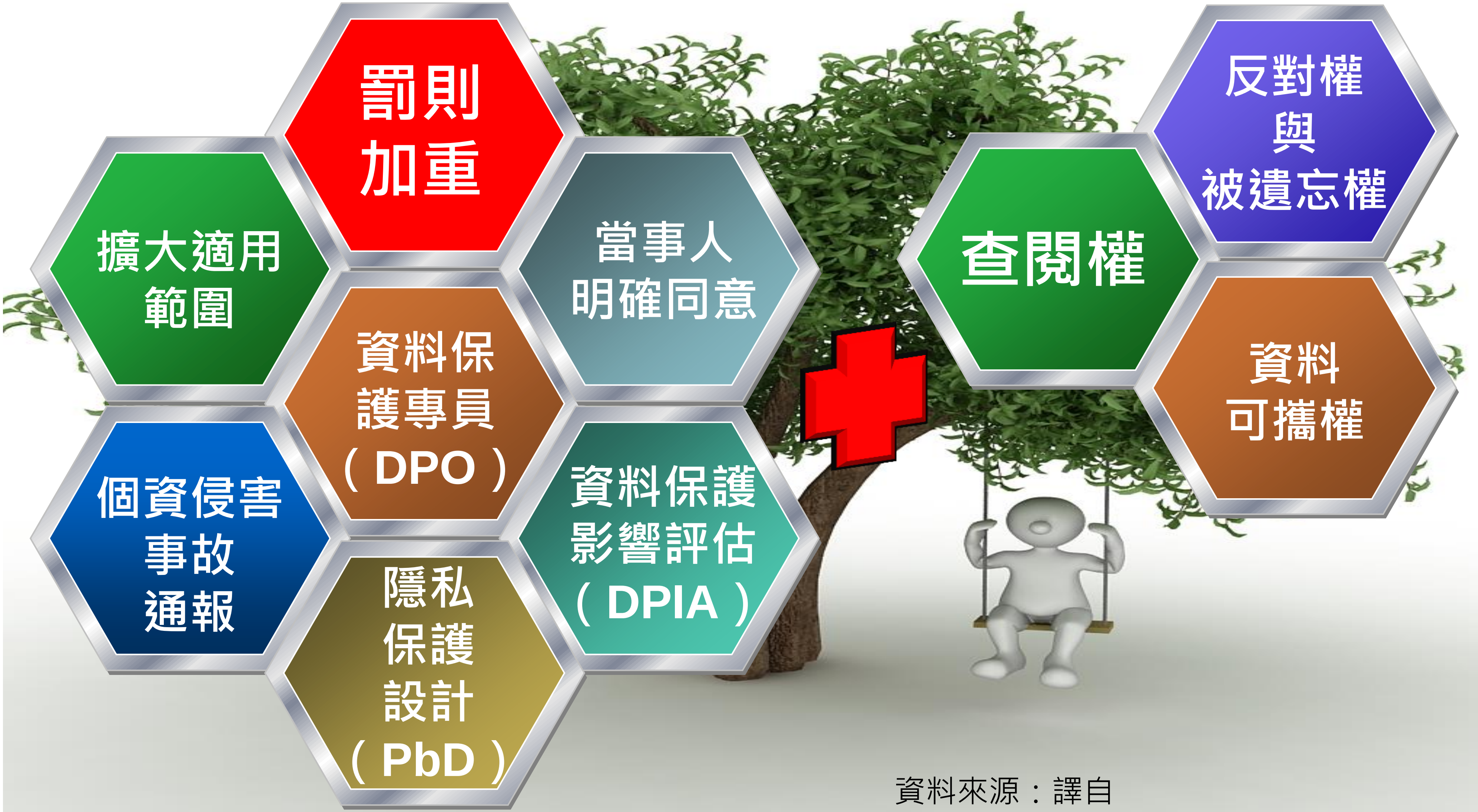
儲存限制性

個人資料不得逾越為處理個人資料的目的之必要範圍（包含儲存期間），在可識別資料主體之狀態下予以保管

完全性與機密性

必須以適當的資訊安全方法確保及處理個人資料，以避免個資遭受無權限或違法之處理，或避免對資料遺失、破壞或損壞

GDPR：規範重點



資料來源：譯自
http://www.eugdpr.org/key-changes.html

GDPR: 規範架構綜覽

- 總則
- 個人資料處理原則
- 資料主體之權利
  - 透明度與管道
  - 個資之資訊與近用權
  - 更正與刪除權
  - 拒絕權與個人化自動決策
  - 權利之限制
- 控管者與處理者的責任
  - 一般義務
  - 個人資料之安全
  - 資料保護影響評估
  - 資料保護官
  - 行為守則與認證
- 個資移轉至第三國或國際組織
- 獨立監管機關
  - 獨立地位
  - 權限、職務與權力
- 合作與一致性
  - 合作
  - 一致性
  - 歐洲資料保護委員會（European Data Protection Board, EDPB）
- 救濟、義務與處罰
  - 個人資料的特殊處理規範

附錄: GDPR規範架構(1/2)

■個人資料處理原則

§5 個人資料處理原則
§6 處理之合法性
§7 個資處理移轉同意條件
§8 涉及資訊社會服務適用兒童同意之條件
§9 敏感個資處理

■建立資料安全程序

§32 處理之安全
§33 向監管機關進行個人資料侵害之通報
§34 向資料主體為個人資料侵害之通知

■ 控管者與處理者義務

§11 不須識別之處理
§25 設計及預設之資料保護
§26 共同控管者
§27 非設立於歐盟境內控管者或處理者之代表
§28 處理者義務
§29 控管者或處理者之處理權限
§30 處理活動的紀錄
§31 與監管機關之合作.

■ 建立資料保護影響評估與事前諮詢制度

§35 資料保護影響評估
§36 高風險之事前諮詢

附錄: GDPR規範架構(2/2)

■資料保護專員設立

§37 資料保護專員之指定
§38 資料保護專員之職位
§39 資料保護專員之職務

■ 建立資料主體權利行使制度

§12 資料主體為使其權利之透明資訊、溝通及管道
§13 蒐集資料主體之個人資料時所提供之資訊
§14 尚未自資料主體取得個人資料時所應提供之資訊
§15 接近使用權、§16 更正權、 §17 被遺忘權、§18 限制處理權
§19 更正或刪除個人資料或限制處理之通知義務
§20 資料可攜權、§21 拒絕權
§22 個人化之自動決策，包括建檔

■ 資料移轉程序

§44 資料移轉之一般原則
§45 基於適當決定之移轉
§46 適當保護措施之移轉
§47 有拘束力之企業守則
§48 未獲歐盟法授權之移轉或揭露
§49 特定情形下之例外移轉

GDPR: 敏感資料

種族、政治意見、宗教、哲學信仰、參與工會、基因、生物特徵資料、有關健康的資料、性生活或性取向

例外允許

- 除歐盟法或會員國法所禁止之外，資料主體已明確同意者；
- 為履行義務及行使控管者特定權利之目的，或資料主體在歐盟法或會員國法或依據會員國法律所訂適當保障資料主體之基本權及利益之團體協約所授權之勞動法及社會安全及社會保護法領域而有必要；
- 為保護資料主體或他人之重大利益，而資料主體於身體或法律上無法表示同意；
- 基金會、協會或任何其他非營利組織，基於政治、哲學、宗教或工會之目的；
- 資料主體已自行公開其個人資料；
- 為建構、行使或防禦法律上之請求權或法院執行其司法權而有必要；
- 為重大公共利益；
- 為預防或職業醫學之目的、為評估僱員之工作能力、醫療診斷、為提供健康或社會照護或治療或為健康管理或社會照護系統及服務而有必要之處理；
- 基於公共衛生領域之公共利益；
- 為追求公共利益、科學或歷史研究目的或統計目的而有必要；
- 公務機關控制下，或歐盟或會員國法以為資料主體之權利與自由規範適當保護措施而授權之處理。且僅限由公務機關控管保存（前科及犯罪之個人資料）。

原則禁止

GDPR：原則禁止跨境傳輸

- **GDPR原則禁止跨境傳輸與資料離境，例外要件（擇一）：**
  - ✓接受國取得「適足性認定」（Adequacy decision）
  - ✓企業自主採行符合規範之適當保護措施：
    - ■資料傳輸方與接收方簽訂經歐盟認可之「標準契約條款」（Standard Contractual Clauses, SCC）。
    - ■「有拘束力之企業守則」（Binding Corporate Rules, BCRs）。
    - ■「行為守則」（Codes of Conduct）
    - ■ 取得特定認證
  - ✓其他例外情形：個資當事人明確同意、執行契約所必要、基於公共利益之重要原因

GDPR：罰則加重（Article 83）

- **最高可處1,000萬歐元或前一年度全球營業總額2%的罰款，取其金額較高者，如：**
  - ✓ 未任命「資料保護專員」（Data Protection Officer, DPO）
  - ✓ 未進行「資料保護影響評估」
  - ✓ 個資外洩等事故發生後，未及時通知監管機關。

- **最高可處2,000萬歐元或前一年度全球營業總額4%的罰款，取其金額較高者，如：**
  - ✓ 未獲當事人充分同意處理個人資料、資料當事人權利之侵害等
  - ✓ 隱私設計（Privacy by Design）核心概念之違反
  - ✓ 違法跨境傳輸個人資料

GDPR:受GDPR規範之企業型態與範圍

- **在歐盟境內設置據點之企業**
  - ✓ 設立母公司、子公司、分公司、事務所、辦事處等據點
  - ✓ 派駐本國或非歐盟員工到歐盟境內的企業

- **未在歐盟境內設置據點之企業**
  - ✓ 對歐盟境內資料主體（居民、消費者等）提供商品或服務
  - ✓ 監控資料主體於歐盟境內活動之行為

GDPR：受影響產業衝擊與挑戰

- **難以掌握個資移轉**：無法掌握企業或集團所有之個人資料處理與移轉狀況。
- **差異難以識別**：無法識別企業或集團現況與GDPR規範要求事項的差異之處，並決定實施對策的優先順位。
- **成本增加**：增加資料保護專員、資料安全防護程序與設備、資料保護影響評估與事前諮詢制度、提供資料主體權利行使制度設立與維運成本支出。
- **來不及**：於GDPR規範適用日（2018 年 5 月 25 日）前無法實施所有對策，恐將面臨相關罰則。


THANK YOU

資料隱私
保護標章

財團法人資訊工業策進會 科技法律研究所

TPIPAS維運暨執行小組

地址：臺北市大安區敦化南路二段216號22樓

◆http://www.TPIPAS.org.tw

◆http://www.dpmark.org.tw

◆TPIPAS臉書粉絲專頁：
https://www.facebook.com/Tawian.TPIPAS/
（或關鍵字「臺灣個人資料保護管理制度 TPIPAS）即可