歐盟一般資料保護規則(GDPR)宣導說明會

日期：107 年 9 月 14 日(星期五)

地點：集思台中文心會議中心 G1 會議室
(台中市西屯區文心路二段 107 號 4 樓)

議程：

時段	主題	講者
13:00~13:30	報到	
13:30~13:45	歐盟一般資料保護規則(GDPR)簡介	國家發展委員會法制協調中心陳嵐君簡任視察
13:45~14:35	GDPR 對產業之影響與因應	資策會科法所戴豪君資深研究員
14:35~14:55	中場休息	
14:55~15:45	【經濟部】經濟部因應 GDPR 施行之策略與作法	經濟部\顏鳳旗副組長
	【金管會】金融業因應歐盟一般資料保護規則(GDPR)施行之相關作為	金管會\李育德副處長
	【交通部】交通部面對 GDPR 之相關因應措施	交通部\林金生科長
	【通傳會】通傳會因應 GDPR 之作為分享	通傳會\林祐仲技正
15:45~16:10	綜合座談	1. 國家發展委員會法制協調中心 2. 資策會科法所戴豪君資深研究員 3. 經濟部\顏鳳旗副組長 4. 經濟部\呂靜忻專員 5. 金管會\李育德副處長 6. 交通部\林金生科長 7. 通傳會\林祐仲技正
16:10~	閉幕式	

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

國家發展委員會

107 年 9 月 14 日

大綱

- 背景
- GDPR 重點
- 跨境傳輸議題分析
- GDPR 對我國企業影響
- 結語

背景

排除會員國間
個資流通障礙

提升個資
當事人權利

強化個資
專責機關權限

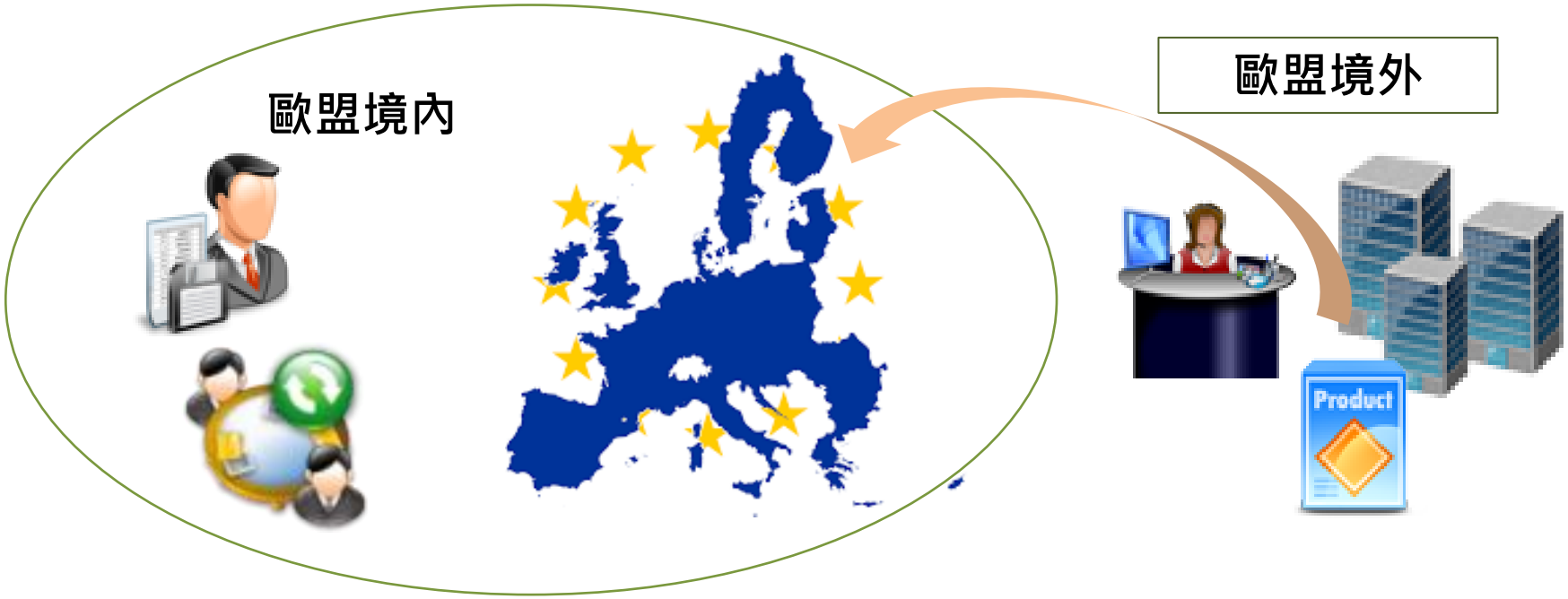
1995
發布「個人資料保護指令」

2016
通過 GDPR
（取代 1995 指令）

2018
5/25 全面實施 GDPR

GDPR
重點

擴大適用範圍

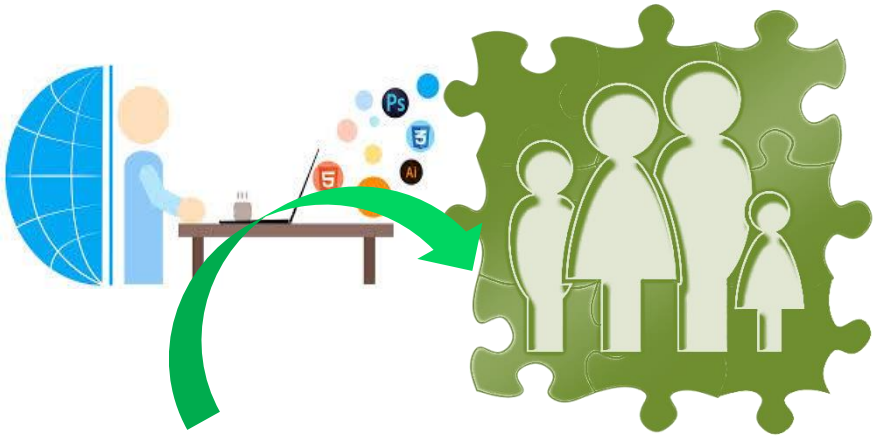


- 設立於歐盟境內之個資處理控管者（data controller）及受託處理者（data processor）；
- 設立於歐盟境外，但對歐盟境內之當事人提供商品或服務、或監控其行為之資料控管者及受託處理者（§3）；此等企業原則應於歐盟設代表，受理相關事宜（§27）

GDPR
重點

擴大個資定義

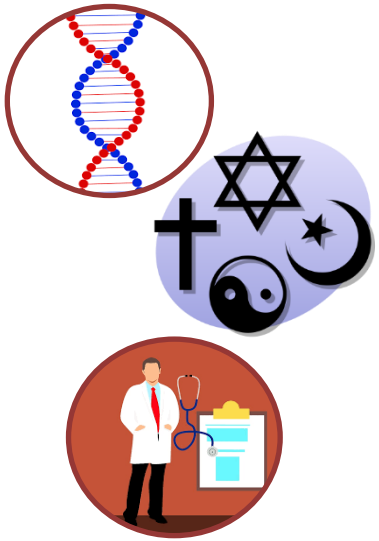
一般個資



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。

GDPR
重點

明確當事人同意

當事人自由提供、具體、知情及明確同意。

不構成同意：

- 單純沉默。
- 預設選項為同意。
- 不為表示。

撤回：
同意之撤回應與給予同意一樣容易。

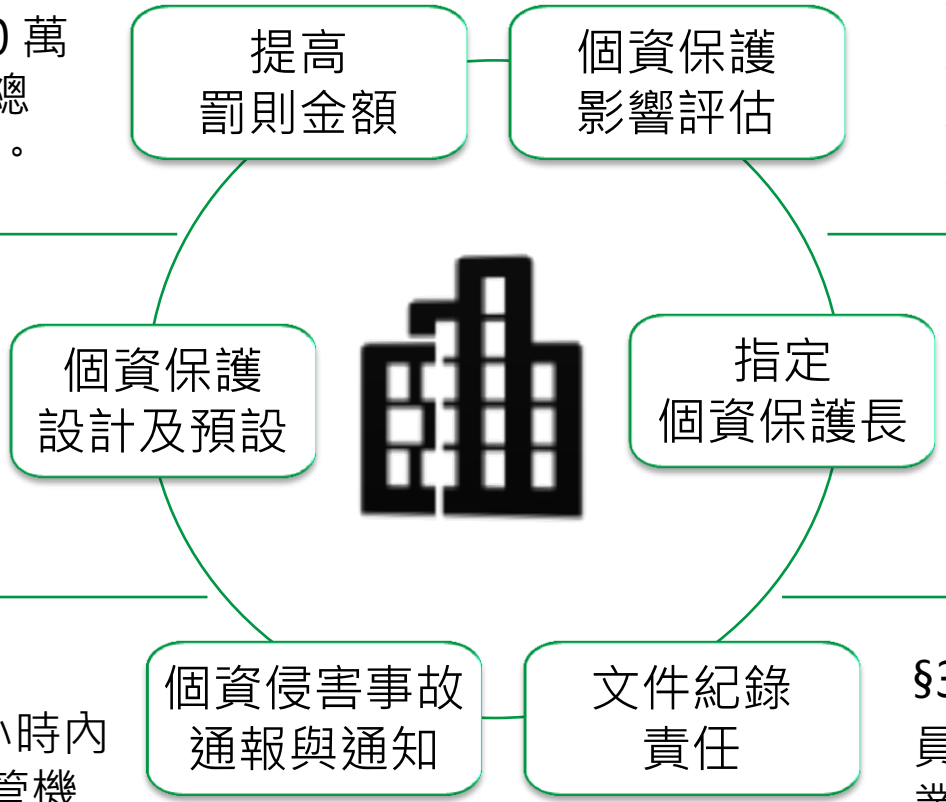
目的：
個人資料之處理具有多重目的者，應就全部目的取得同意。

GDPR
重點

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。

§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。



§24
在技術上及組織上納入隱私保護措施。

§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。

§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。

§30
員工 250 人以上企業原則應保存維護相關紀錄。

GDPR
重點

強化當事人權利

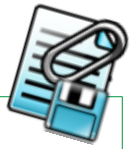
§ 21、22
當事人應有權拒絕對於自動化決策或以任何形式評估個人特徵之建檔行為。

更正權

§ 16
當事人有權使控管者更正其不正確之個資，且有權補充其個資。

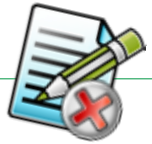
拒絕權

刪除權
(被遺忘權)



§ 20
當事人有權要求以結構的、通常使用的、機器可讀形式，接收其原提供予控管者之個資，並有權傳輸予其他控管者。

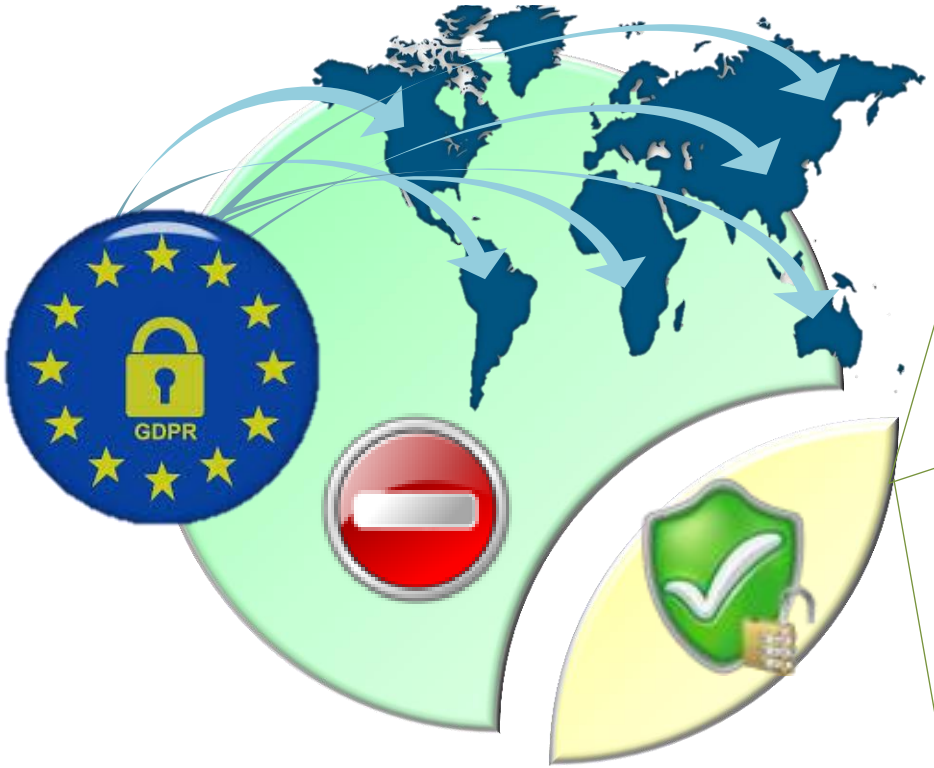
個資
可攜權



§ 17
個資蒐集、處理目的消失，或遭違法處理，當事人得請求刪除其個資或連結。

GDPR
重點

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）

其他排除適用情形：
例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

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
- 其他排除適用情形

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。

跨境傳輸
議題分析

企業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）	• 歐盟企業跨境傳輸多採行此方式 • 目前版本仍為 95 指令時代所公布
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。
行為守則（Codes of Conduct）	• 鼓勵特定行業、中小企業、微型企業等採行。 • 由公協會或代表特定資料處理活動之機構申請。
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。 • 適合採用之企業：業務僅涉及特定業別。

其他排除適用情形

- 跨境傳輸應優先採行上述國家層級適足性認定，或企業自主採行適當保護措施方式。
- 於少量、偶發性之傳輸時，可採以下方式。

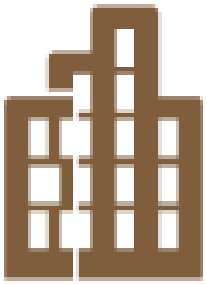
其他例外情形	內容
個資當事人明確同意	告知個資當事人可能之風險後，取得當事人明確同意移轉。
其他必要措施	例如： • 因執行契約所必要。 • 基於公共利益之重要原因。 • 於個資當事人無法為同意之表示，移轉對其有重要利益保護必要。

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，或符合其他排除適用情形。

GDPR 對我國企業之影響

影響程度



• 非設立於歐盟境內	⟷	• 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。
• 偶然性處理歐盟個資	⟷	• 大規模處理歐盟個資
• 於歐盟境內處理個資	⟷	• 進行跨境傳輸
• 使用一般電子處理	⟷	• 使用大數據分析或雲端服務
• 在歐盟經濟活動規模較小	⟷	• 在歐盟經濟活動規模較大

結語

國發會統籌GDPR事宜

歐盟為全球重要經濟體，並為我國第 5 大貿易夥伴，面對 GDPR 的施行，需整合相關部會作為，以協助企業因應：

- ✓ 官網建置 GDPR 專區。
- ✓ 各目的事業主管機關提供企業諮詢輔導。
- ✓ 國發會會同相關機關辦理適足性認定事宜。


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

結語

國發會成立個人資料保護專案辦公室

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

簡報結束

附件

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。

附件

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。

附件

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。

歐盟一般資料保護規則(GDPR)北中南宣導說明會

GDPR對產業之影響與因應

- 資訊工業策進會科技法律研究所
- 戴豪君
- 2018.09
- irving@iii.org.tw

報告大綱

- 前言
- 歐盟GDPR規範重點與影響
- 企業因應GDPR之作法
- 因應GDPR之相關資源

GDPR是歐盟20年來隱私保護最重大變革

Andrea Jelinek, Chair of the EDPB

This much awaited legislation gives individuals greater control over their personal data and provides a single set of rules applicable to everyone processing the personal data of individuals in the EU.

In a world where data is treated as a currency, the rights of individuals were often overlooked or even flouted.

We should not lose sight of the fact that personal data are inherent to human beings.

I am convinced that the GDPR gives individuals and supervisory authorities the means to effectively protect and enforce this fundamental right.

25 May,2018

資料來源：https://www.eugdpr.org/eugdpr.org-1.html

資料創新應用帶動資料經濟

公共領域
- 普查、稅務、醫療等

金融
- 顧客行銷、風險分析等

製造業
- 研發、營運

零售
- 客戶行銷、營運、線上銷售

電信
- 客戶電話紀錄、詐騙行為分析等

醫療
- 病歷、醫療研究、消費行為等

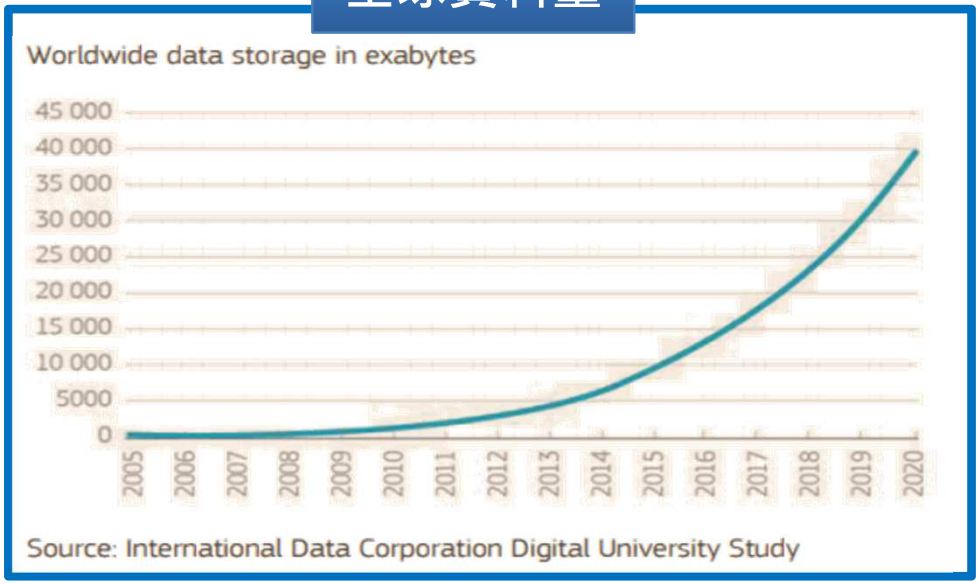
歐盟2017年新資料經濟(Data Economy)策略

資料為基礎的產品與服務（Digital data-based products and services）是農業、食品安全、氣候、智慧城市、能源等轉型契機，例如企業引進數據支持之決策程序效能可提高6 %

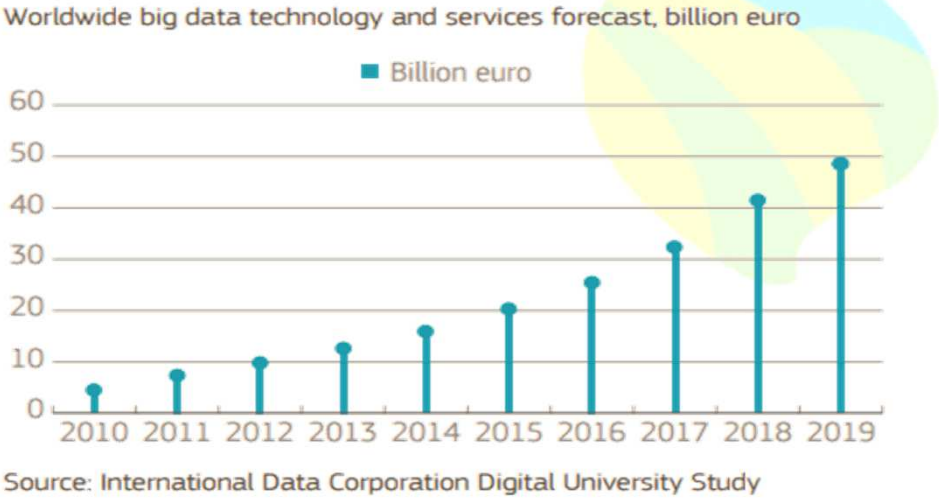
資料來源：資策會MIC (行業別巨量資料分析應用方向)，2017年6月16日

歐盟資料經濟政策

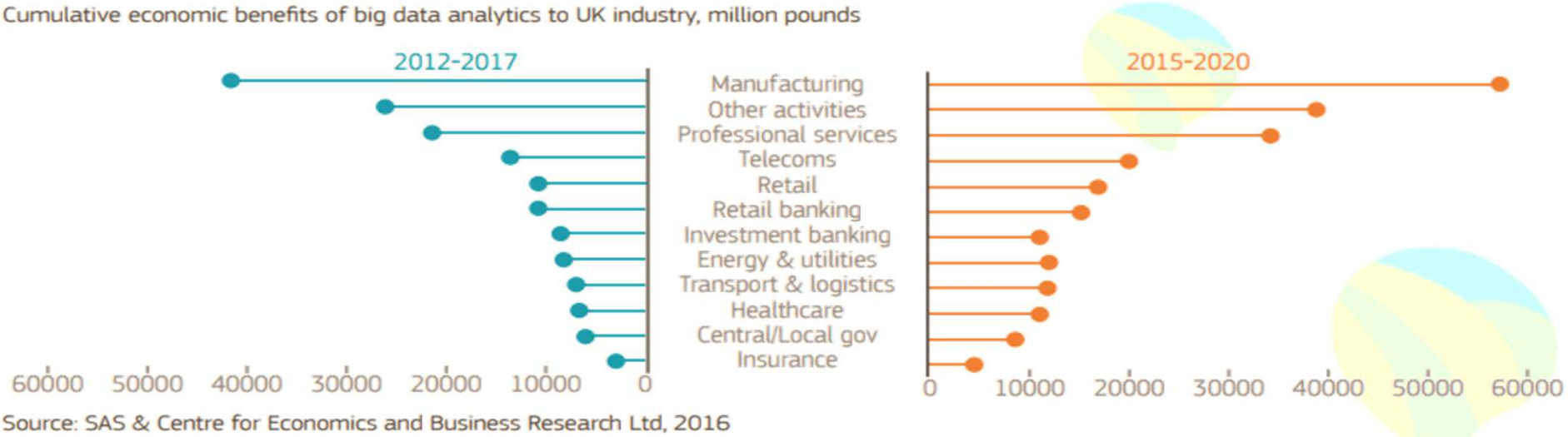
全球資料量



歐盟預估境內資料經濟至2019年將達4370億歐元



愈來愈多行業擁抱資料金礦



資料來源：歐盟政治策略中心「歐盟資料經濟政策」(Enter the Data Economy)，2017年

迎向GDPR：企業變更營運策略

臉書規避歐盟新個資規範 15億用戶資料將搬回美國

2018-04-21 21:20

〔即時新聞／綜合報導〕「資料保護規範」（General Data Protection Regulation，GDPR）5月將在歐盟國家施行，這次變動號稱是歷來最嚴格的個資保護法，違反規定的企業最高可罰全球營業額的4%。據外媒報導，臉書趕在5月25日歐盟新法生效之前，將美國、加拿大、歐洲地區之外的15億用戶資料從愛爾蘭移至美國，避免受到GDPR管轄，預估有超過70%用戶受影響。

倫敦大學學院（UCL）科技政策研究員韋爾（Michael Veale）表示，移出使用者資料意味著臉書將受到較寬鬆的美國隱私權規範。根據歐盟法律，瀏覽歷史紀錄會被視為個人數據，在美國則不受保障。臉書因此採取將非洲、亞洲、澳洲與拉丁美洲的用戶資料移至美國的策略，以規避歐盟新法。這將影響到15億用戶的權利，也減少了對隱私權的保障。

資料來源：http://news.ltn.com.tw/news/world/breakingnews/2402523 (last visited May. 11, 2018).

設停損點：企業終止對歐洲客戶服務

GDPR效應：美國部份媒體為自保，限制歐洲民眾存取

《歐盟通用資料保護規則》（EU General Data Protection Regulation，GDPR）在上周五（5/25）正式實施了，儘管各大業者皆兢兢業業地部署符合GDPR的隱私條款，但臉書（Facebook）與Google還是在該規範上路的第一天就被告了，而美國媒體洛杉磯時報（LA Times）與芝加哥論壇報（Chicago Tribune）則是在上周五開始拒絕歐洲用戶存取，目的是為了規避GDPR。

與其企圖闖關，這些媒體選擇了明哲保身。GDPR闡明所有歐洲民眾都有權檢視企業所握有的個資，而且還能要求企業刪除這些個資，企業除了必須取得蒐集與使用個資的明確同意之外，也必須在發生資料外洩事件的72小時內通知使用者與主管機關。

然而，臉書與Google之所以被告卻是因為這些同意書，他們要求使用者同意[illegible]服務條款否則便無法使用相關服務，使用者認為他們是「被迫同意」的[illegible]陷入了兩難的局面。

Los Angeles Times

資料來源：https://www.ithome.com.tw/news/123466 (last visited May. 11, 2018).

企業陸續調整隱私權政策

GDPR and updates to our privacy policy

The Boomerang Team boomerang@baydin.com

You've probably gotten an awful lot of emails over the past few weeks about privacy policy updates due to the GDPR -- here's one more from us!

Cookie Name Description of purpose. More information. When do cookies expire 1st party or 3rd party cookie?

Cookie Name	Description of purpose. More information.
Snapengage	Used for real-time chat functionality with visitors of our websites and through the Boomerang Apps.
Boomerang login cookie	Used for authentication of Boomerang users

資料來源：http://boomerangapp.com/cookiepolicy.html (last visited May. 11, 2018).

EDPB與各行業進行GDPR之調適

European Data Protection Board

edpb European Data Protection Board

HOME ABOUT EDPB

European Data Protection Board > News > News > Letter to ICANN

Letter to ICANN

Thursday, 5 July, 2018

The EDPB adopted a letter on be
(ICANN), providing guidance to e
context of WHOIS.

The letter addresses the issues c
access to non-public WHOIS data

The EDPB's predecessor, WP29, h
protection law since 2003.

The EDPB expects ICANN to deve
such as law enforcement, of pers

European Data Protection Board

edpb European Data Protection Board

HOME ABOUT EDPB

European Data Protection Board > News > News > Letter regarding the PSD2 Directive

Letter regarding the PSD2 Directive

Thursday, 5 July, 2018

The EDPB adopted a letter on behalf
Directive (PSD2 Directive). In its repl
the procedures with regard to giving
and the European Commission, EDPS

PSD2 Letter 4.86 MB

圖片資料來源：https://edpb.europa.eu/

報告大綱

- 前言
- 歐盟GDPR規範重點與影響
- 企業因應GDPR之作法
- 因應GDPR之相關資源

GDPR之適用範圍

01

人

在歐盟境內的任何個人資料；公、私部門均有適用

02

地區

以歐洲經濟區(EEA)設有據點為主，但在境外亦有可能

03

行為

個資「處理」或「移轉至境外」

04

資料

姓名、識別號碼、住址、電子郵件地址、IP/cookie、其他

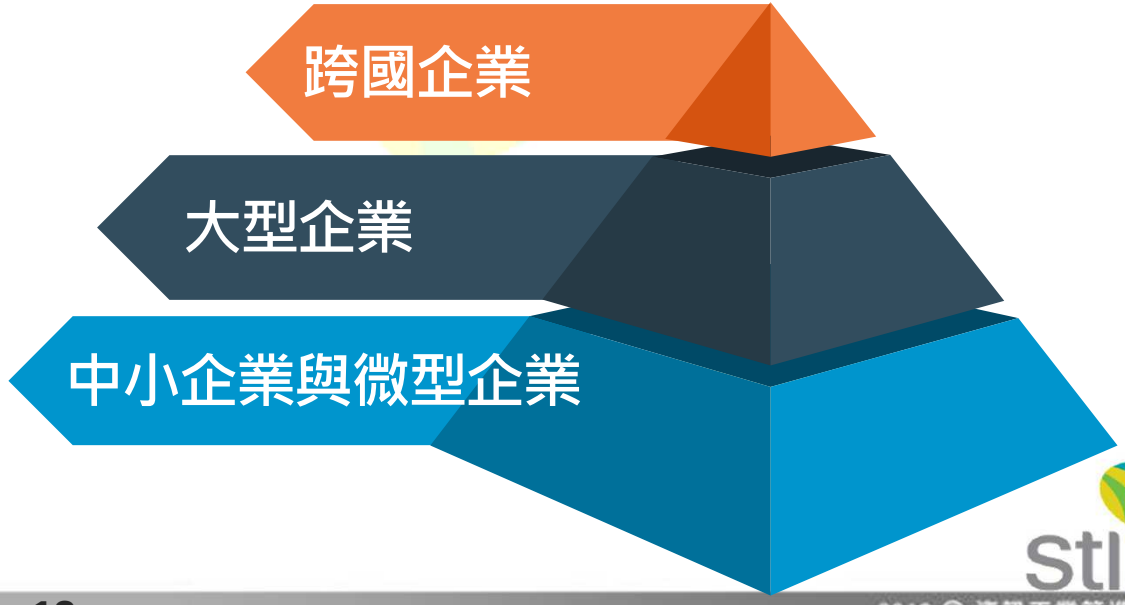
GDPR之適用範圍

GDPR於下列範圍不適用- Art.2

- 於歐盟法律治權領域外之活動
- 會員國所進行屬於歐盟條約第V篇第2章共同外交與安全政策之活動
- 當事人(data subject)單純之個人或家庭活動
- 歐盟機關、機構、辦事處及局處之資料處理以及該等資料之流通，關於當事人保護之規範
- 主管機關為達預防、調查、偵查或追訴刑事犯罪或執行 刑罰目的，所進行之個人資料處理
- 不影響資訊社會服務指令(Directive 2000/31/EC)有關 單純傳輸、暫存、主機服務等，ISP業者無監督義務之規定

GDPR規範適用的企業型態與範圍

- 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、辦事處等據點的企業
  - ✓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企業
  - ✓對歐盟境內資料主體提供商品 或服務的企業
  - ✓在歐盟境內監控資料主體於歐盟境內行動的企業



受GDPR規範影響的產業營運項目例示

貨物產業	服務產業

• 電機、機械、鋼鐵、汽車、醫藥
  • 人力資源：駐歐盟據點或到歐盟出差人員的人事資料
  • 客戶諮詢：歐盟客戶個資
  • 行銷服務：歐盟客戶(含法人代表人)個資
  • 資料備援與管理：客戶個資與人事資料處理與移轉
  • 藥品測試：藥品受測者個資
  • 各部門：前述個資處理與移轉(含跨國傳輸)
	• 運輸、商業、旅遊、金融服務
	  • 人力資源：駐歐盟據點或到歐盟出差人員的人事資料
	  • 運輸/商業/旅遊/金融/保險(附加)/電信服務：歐盟客戶個資
	  • 客戶諮詢：歐盟客戶個資
	  • 服務行銷：歐盟客戶個資
	  • 資料備援與管理：歐盟客戶個資與員工個資
	  • 各部門：前述個資處理與移轉(含跨國傳輸)

GDPR規範架構總覽

修正個人資料處理原則

- §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(16歲)同意之條件
- §9特種個資處理

新增控制者與處理者義務

- §11不須識別之處理
- §25設計及預設之資料保護
- §26共同控制者
- §27非設立於歐盟境內控制者或處理者之代表
- §28處理者義務
- §29控制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溝通

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 (DPIA)
- §36高風險之事前諮詢

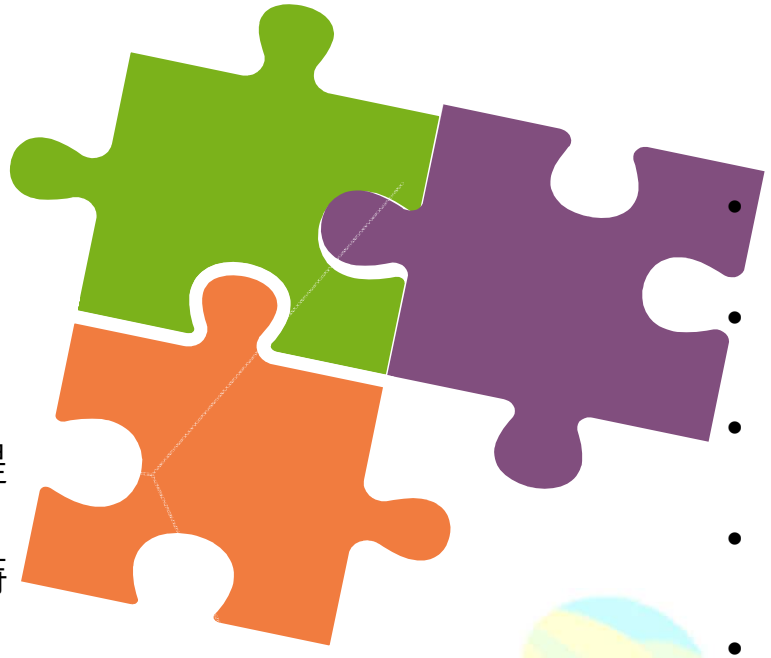
GDPR規範架構總覽

資料保護專員(DPO)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



修正資料傳輸程序

- §44資料傳輸之一般原則
- §45基於適當決定之傳輸
- §46適當安全保護措施之傳輸
- §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重點

重點綜覽			
適用範圍更廣	增訂資料控制者等之義務	強化資料當事人之權利	提高資料保護責任
• 對象：含資料控制者(data controllers)及資料處理者(data processors) • 地域：國外處理、提供服務或監控歐盟人民資料之機關亦適用 • 自然人：16歲以下兒童的資料處理，應取得家長同意	• 資料保護衝擊影響評估(DPIA) • 隱私設計(PbD) • 事故通報義務 • 歸責(accountability)及遵循要求 • 當事人明確而肯定的同意（clear and affirmative consent） • 資料剖析(profiling) • 特定情況應設置資料保護專員(DPO)	• 強化通知條件 • 資料可攜權(data portability) • 被遺忘權(right to be forgotten) • 限制資料處理權利	• 行政罰鍰可能至全球總年營業額4% 或 2,000萬歐元，從重 • 一站式機制強化會員國個資監管機關執行權限

當事人得行使之權利

01 近用權

02 訂正權

03 刪除權（被遺忘權）

04 限制處理權

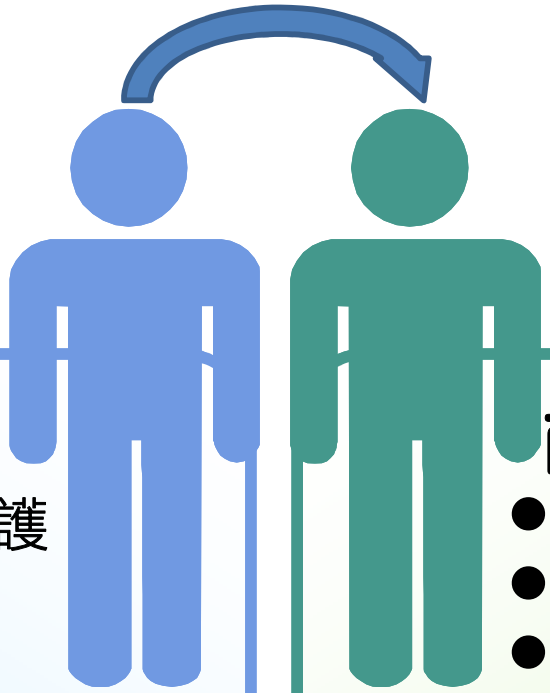
05 資料可攜權

06 拒絕權

07 自動化決策權

控管者與處理者責任之差異

處理權限 Art.29



控管者（Controller）
基本責任 Art.24,26

處理者（Processor)
基本責任 Art.28

僅限控管者之規範

- 應進行設計及預設之資料保護 **Art.25**
- 向主管機關通報個資侵害 **Art.33**
- 向當事人溝通個資侵害**Art.33**
- 依規進行**DPIA**與事前諮詢 **Art.35,36**

兩者相同規範

- 非設立歐盟境內之代表 **Art.27**
- 處理活動之記錄 **Art.30**
- 個人資料處理之安全 **Art.32**
- 資料保護員 **Art.37**
- 確保適當保護措施移轉個人資料至第三國或國際組織 **Art.46**
- 司法救濟、損害賠償與行政罰

GDPR重點摘要說明(1/4)

一、資料控制者(data controllers)之定義

判定資料處理之目的及方法之自然人或法人、公務機關/機構/單位，對資料提供與否、資料提供範圍與形式、資料使用目的有決定權

二、資料處理者(data processors)之定義

受資料管理者指示，處理資料之自然人或法人、公務機關/機構/單位

[增訂資料控制者等之義務]

一、資料保護衝擊影響評估(Data Protection Impact Assessment, DPIA)

在歐盟境內處理、利用資料並非一定要進行資料保護衝擊影響評估。依GDPR第35條，資料處理、利用行為如有法定要求，或涉及高風險，抑或處理方法顯著變更時，須進行衝擊影響評估

二、隱私設計(Privacy by Design, PbD)

資料控制者在設計處理系統以及運用該系統時，為保護資料當事人的權利，確實遵守GDPR，必須採取適當的技術以及相關的組織措施。除此之外，對照處理個人資料目的之必要性，個人資料應具有適當性、具有關聯性，並且僅限在最小限度內

三、事故通報義務

公司、機構須於知悉外洩時起72小時內，通知主管機關有關於個資洩漏情事，並於第一時間通知資料當事人所有狀況使其了解嚴重性，讓資料利用者得採取適當措施因應

GDPR重點摘要說明(2/4)

四、資料剖析(profiling)

任何針對個人資料之自動化處理形式，凡自動化處理以分析、預測特定自然人之工作表現、經濟狀況、健康、個人偏好、興趣、信用、行為、位置或移動等，均屬GDPR下之資料剖析。

五、設置資料保護專員(Data Protection Officer, DPO)

在以下幾種情形下的組織，DPO是被強制要求設置

- 公部門：公務機關或團體進行資料的處理時（法院作為司法機關的行為除外）
- 業務屬性：核心性業務為有必要大規模地，定期且有系統的監視資料當事人處理作業之情形
- 資料類型：管理者或處理者的核心性的業務，為大規模地處理屬於敏感個人資料之情形

[強化資料當事人權利]

一、資料可攜權 (data portability)

「資料可攜權」使當事人得於服務提供者間傳遞其個人資料。使個人資料更容易被資料當事人所取得，當事人更可以瞭解其資料被處理之情形，且可以更簡單明瞭地方式取得其個資。

二、被遺忘權 (right to be forgotten)

個人不再希望其個人資料被處理，並表示資料控制者對於資料不再具合法目的，資料將會被刪除。

「被遺忘權」之目的，係保護個人隱私權，而非消除過去紀錄或者限制言論自由。

GDPR重點摘要說明(3/4)

[提高資料保護責任]

一、罰款

- 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：未任命DPO、未進行DPIA或個資事故發生卻未及時通報監管機關者
- 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：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

二、當事人申訴與司法救濟

- 當事人其有關之個人資料處理違反本GDPR者，當事人有權向主管機關提出申訴（Art.77）
- 自然人或法人有權對主管機關對其所為具有拘束力之處分，以及其個人受資料控管者或處理者侵害時，得提起司法救濟（Art.78-79）

三、賠償請求權

- 任何人因違反本規則之行為，而受物質上或非物質上之損害(material or non-material damage)，應有權利向控管者或處理者請求損害賠償
- 控管者或處理者之責任範圍，以及共同控管者的連帶損害賠償責任（Art.82）

GDPR重點摘要說明(4/4)

[提高資料保護責任]

四、類似團體訴訟之當事人代表

- 依會員國法合法設立、以公益為目的且在個人資料保護領域活躍之非營利機構、組織或社團，得受委託代其向主管機關提出申訴、代其行使行政、司法救濟之權利，於會員國法有規定時，可代其行使收受賠償金之權利。（Art.80）

五、一站式機制：

- GDPR為了實現資料單一市場，除了訂定同樣規範，歐盟也同時希望達到規範同一施行。第127條規定一站式機制，如果爭議事件之資料管控或資料處理所在地包括歐盟內部數個會員國，爭議得提交至其中主要監管機關(lead supervisory authority)進行爭端解決，判決內容對於歐盟其他相關會員國具影響力(implications for all of Europe)。因此，歐盟之跨國公司僅需面對一個監管機關，而非28個會員國之監管機關。

我國個資法與GDPR之比較(1/3)

	我國個資法	GDPR	比較及建議
當事人告知及同意	✓不限方式 ✓當事人經蒐集者告知應告知事項後，所為允許之意思表示	✓ 不限方式 ✓ 易懂且方便取得之格式 ✓ **清楚簡易之語言**	就同意取得而言，GDPR特別說明應以易懂格式、簡易語言等方式，組織應特別注意
資料保護專員(DPO)	我國僅在施行細則第12條2項1款有類似規定 一、配置管理之人員及相當資源	第37-39條規定職務內容及設置條件 ✓ **公務機關進行個資處理** ✓ 須定期且大規模監控資料當事人 ✓ 處理特殊類型個資	我國個資法並無強制要設置，惟GDPR規定只要符合特定情況則一定要設立，並設有相關之設置條件

我國個資法與GDPR之比較(2/3)

	我國個資法	GDPR	比較及建議
當事人權利	✓查詢、請求閱覽 ✓取得複製本 ✓補充或更正 ✓要求停止蒐集、處理或利用 ✓要求刪除	✓資料近用權 ✓資料訂正權 ✓資料刪除權 ✓資料限制權 ✓資料可攜權 ✓資料異議權	GDPR賦予當事人之權利範圍較我國個資法為廣，以近用權為例，甚至涵蓋應提供得遠端使用之安全系統供資料當事人使用；並多賦與資料可攜權及針對自動化處理得行使拒絕權
自動化處理之限制	無	✓資料當事人得行使拒絕權 ✓資料控制者須有權為部分介入	此為GDPR獨有之限制，組織應特別注意是否符合例外情況，若否，則應注意要如何落實本條之要求

我國個資法與GDPR之比較(3/3)

	我國個資法	GDPR	比較及建議
個資違反通報	✓適當方式通知資料當事人 ✓若相關法規或主管機關有要求則須向主管機關通報	✓通報監管機關，必要時通知資料當事人 ✓72小時內通報，若無需通知遲延之理由	GDPR規定較為嚴格，我國僅於部分子法中對於通報主管機關有規定，應特別留意
跨境傳輸	**原則允許、例外禁止**	**原則禁止、例外允許** ✓傳輸至充分符合GDPR規範之國家(適足性認定) ✓採取適當安全措施如共同約束規則(BCR)、標準契約條款(SCC)等 ✓取得資料當事人同意	與我國個資法相反須符合列舉情況始得跨境傳輸，因此組織應注意是否落實列舉事由
罰則	✓刑事責任 ✓民事責任 ✓行政責任(罰鍰最高50萬)	✓民事責任 ✓行政責任(視情況罰鍰最高可達2000萬歐元或4%全球營業總額)	GDPR可能之裁罰金額極高，為避免被裁罰組織應特別注意規範事項

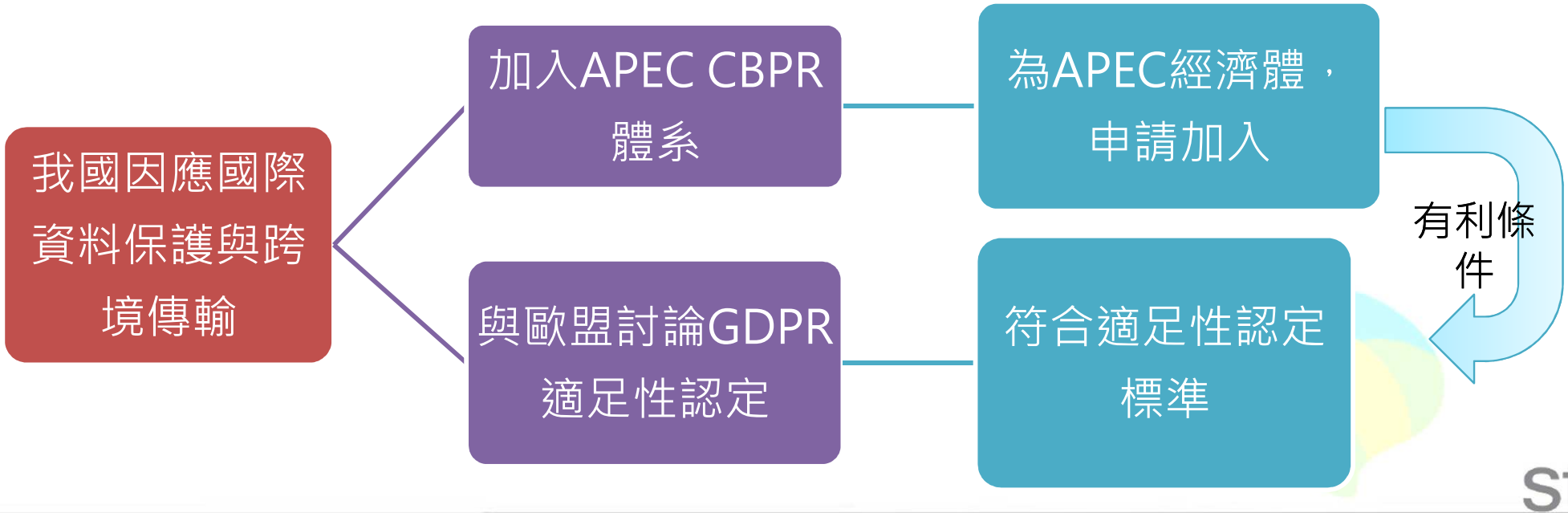
GDPR允許個資跨境情況

- 國家層次：國家通過適足性認定(adequacy decision)
- 企業自我規律：企業採取適當安全措施，確保個資跨境傳輸合於GDPR
- GDPR特別規定(derogations)：企業個資跨境傳輸符合GDPR第49條特別規定 (例如，取得當事人同意等)，參見 Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679

國家層次：GDPR適足性認定

歐盟執委會評估時考量下列因素(歐盟GDPR第45條第2項)

- 對人權與基本自由之尊重與相關國內法規範(rule of law)：主要對應我國個資法
- 有獨立有效運作之監管機關(independent supervisory authority)：必須溝通**我國個資目的事業主管機關的特殊性**
- 與第三國或國際組織之國際承諾(international commitment)或其他有關資料保護的義務(來自公約或參與相關多邊、區域體系)：確認我國國際性資料保護承諾進程(例如：加入APEC CBPR體系)



國家層次：歐美隱私盾協議(Privacy Shield Agreement)

歐盟法院(CJEU) Case C-362/14, Schrems vs. Data Protection Commissioner ：應確保個人基本權與自由之保護；與指令所提供之保護**實質上相等(essentially equivalent)**，而該國所提供之法律保護必須有效

2015/10歐盟法院判決歐美安全港無效

2015/12 歐美協商安全港替代方案

2016/7 歐美協商完成隱私盾協議（EU-U.S. Privacy Shield）

2017/10 歐盟執委會完成首次隱私盾之年度審查

2017/11 WP29提出報告

2018/5 GDPR施行

截自2018/3/7共有2769家組織加入

日、韓經驗：GDPR適足性認定進展

(2017/11)韓國通訊委員會(KCC)與資訊安全署(KISA)與歐盟討論加強韓國-歐盟間資料保護與流通

歐盟執委會鼓勵韓國成為《自動化處理個人資料保護公約》(Convention 108)觀察員。

確認修改相關立法使資料保護體系相容

2018/5歐盟境外已有12個經濟體通過適足性認定(adequacy decision)

(2013)啟動日本-歐盟經濟夥伴協定(EPA)談判，含資料保護

(2017/12)個人情報保護委員會(PPC)與歐盟針對相互適足性認定(mutual adequacy findings)發表共同聲明

(2017/12)PPC提出個人情報保護法(APPI)第24條資料跨境傳輸修正草案，增加外國適足性認定判斷標準，(2018/1)完成公眾諮詢

(2018/2)PPC將提出資料傳輸歐盟指引

(2018/4)日本-歐盟EPA提交歐盟理事會，啟動歐盟批准程序

確認APPI與GDPR概念相容性與主要差異，包含：**敏感性個資定義、當事人權利、資料使用目的範圍釐清、資料從日本再傳輸至歐盟以外國家、匿名化資料**等
其他差異：**設置DPO要求、安全事故通知、資料剖析、資料可攜性**等

策略：以EPA達成

企業自我規律：適當安全措施

◆企業自主採行符合規範之適當安全措施（Art.46）

1. 具拘束力企業規則（Binding Corporate Rules , BCRs）
   - 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，移轉個資之保護政策
2. 資料傳輸方與接收方簽訂經歐盟認可標準資料保護條款（Standard Data Protection Clauses, SDPC）
3. 行為準則（Codes of Conduct）
   - 應考量特定行業之微型及中小型企業特定需求
4. 取得特定認證
   - 歐盟層級之認證尚未見，部分歐盟會員國有認證機制

➢ 特別規定：當事人明確同意、履行契約或依當事人要求，為締約前之必要措施（Art.49）

法遵方向1：具拘束力企業規則 (BCRs)

◆企業向主管機關申請具拘束力企業規則（Binding Corporate Rules , BCRs）Art.47

- BCRs效力範圍可及於從事共同經濟活動（ a joint economic activity ）集團內所有企業
- GDPR簡化企業申請BCRs程序，改由主管機關遵循一致性原則決定

◆ 申請主體與文件

- 該集團歐洲總部的所在地，或該企業負責處理個人資料保護部門所在地。或負責執行BCRs的部門所在地等
- 符合WP 29工作小組公佈 WP 256號文件等規範

法遵方向2：標準契約條款(SCC)

◆歐盟針對個人資料標準契約條款（ standard contractual clauses, SCC）發布不同類型範本

- ➢規範歐盟控制者（ EU controller）傳送資料到非歐盟或歐洲經濟區控制者（ non-EU or EEA controller）
  - **decision 2001/497/EC**
  - **decision 2004/915/EC**
- ➢ 規範歐盟控制者傳送資料到非歐盟或歐洲經濟區處理者（ non-EU or EEA processor）
  - **decision 2010/87/EC**

法遵方向3：行為準則

◆鼓勵特定行業與中小企業與微型企業遵循行為準則（Codes of conduct）Art.40

- 行為準則的內容應包括： 公正及透明之資料處理、 個人資料之蒐集、 個人資料假名化、提供大眾及當事人之資訊、 當事人權利行使方式、資料安全與隱私設計、受侵害時通報與通知、個人資料移轉至第三國或國際組織等

➢現有行為準則例示

- 歐盟層級： European code of practice for the use of personal data in direct marketing issued by FEDMA
- 會員國層級： German Insurance Association issued Code of Conduct

法遵方向4：取得特定認證

◆主管機關、EDPB及執委會應鼓勵，建立歐盟層級資料保護認證機制與資料保護標章及標誌（data protection seals and marks）Art.42,43

- ➢認證應係志願申請，並透過透明程序取得，取得認證，最長期限應為三年得重新更新
- ➢現有的認證機制如：ePrivacyseal EU 、EuroPrise、CNIL Labels、PrivacyMark system等
- ➢Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679
- ➢

資料跨境傳輸可能面臨問題：資料在地化

資料跨境傳輸法律議題，在於各國個資保護規範程度差異

各國資料跨境傳輸限制與否：資料在地化(Data localization)

- 要求企業應物理上儲存與處理資料於國內之伺服器

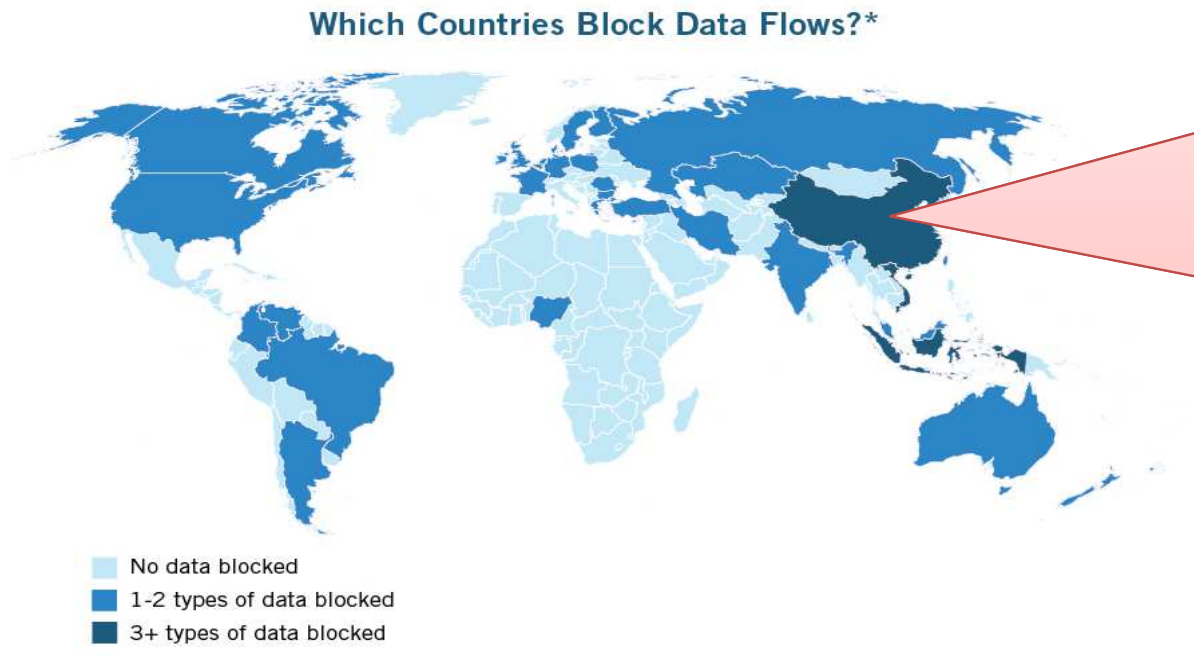
資料在地化政策正當目的

- 隱私與網路安全←無論資料儲存在何處都可能有**資安風險**，重點應為服務提供者之資安保護技術與資料管控
- 扶持產業發展←**數位重商主義(Digital Mercantilism)**
- 國家安全或監管

資料在地化措施

- 如規定禁止企業將特定資料(如個資、敏感資料等)傳輸至境外、於一定期間於境內保留特定資料、類似於歐盟規範原則禁止跨境傳輸，除非傳輸至第三國符合適當保護水準之要求，其他如有當事人同意、契約約定、法律明定事由...等

全球資料在地化實施國家



資料來源：Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?, Nigel Cory(ITIF)

中國(圖中顏色最深)資料在地化規範多明文規定

如：網絡安全法第37條、個人資料和重要資料出境安全評估辦法(徵求意見稿)第2條、中國人民銀行關於銀行業金融機構做好個人金融資料保護工作的通知第6條、網絡出版服務管理規定第8條、人口健康資料管理辦法(試行)第10條、徵信業管理條例(國務院令第631號)第24條、反恐怖主義法第19條

- 目前國際上多**未以資料在地化直接明文規定**，但會**規定跨境傳輸**，於特定條件下，始得進行資料跨境傳輸，如歐盟規定資料接收國應提供個人資料適當保護水準，或提供適當的安全維護措施，且資料當事人權利可以執行並有效救濟途徑存在
- 未來資料傳輸需求大，跨境傳輸國際趨勢更應思考**促進資料自由流通之友善而值得信賴之安全環境**

報告大綱

- 前言
- 歐盟GDPR規範重點與影響
- 企業因應GDPR之作法
- 因應GDPR之相關資源

因應GDPR實施我國整體措施

各部會積極協助所轄產業相關輔導與諮詢服務

- 我國受GDPR實施影響最大的前三個產業依序是**金融業(特別是在歐盟設置據點的八大公股行庫)**、**電子商務**以及**航空公司**。金管會、經濟部以及交通部等相關部會，都已著手輔導企業符合相關的規定

成立個資保護專案辦公室協調各部會GDPR因應事宜

- 我國個資法未設單一主管機關而採分散管理制度，行政院指示國發會於2018年7月4日正式成立「個人資料保護專案辦公室」，以協調整合部會辦理GDPR相關因應事宜

洽談適足性認定

- 國發會五月底拜訪歐盟執委會GDPR的主政官員，表達台灣取得適足性認定的意願

台灣通過APEC跨境隱私保護體系CBPR第一階段審查

- 台灣於2018年5月21日通過APEC跨境隱私保護體系（CBPR）第一階段審查。APEC也正在力推與歐盟GDPR接軌互通，我國若能加入CBPR體系，將有助於我國業者進一步整備符合歐盟標準

現階段企業因應重點

1. 判斷是否適用GDPR
2. 評估是否選任歐盟代理人(Art. 27)
3. 合法處理個人資料
4. 依GDPR之法定要件進行個資跨境傳輸
5. 備妥事故因應程序

個資相關問題判斷流程

■ 個資法問題判斷核心

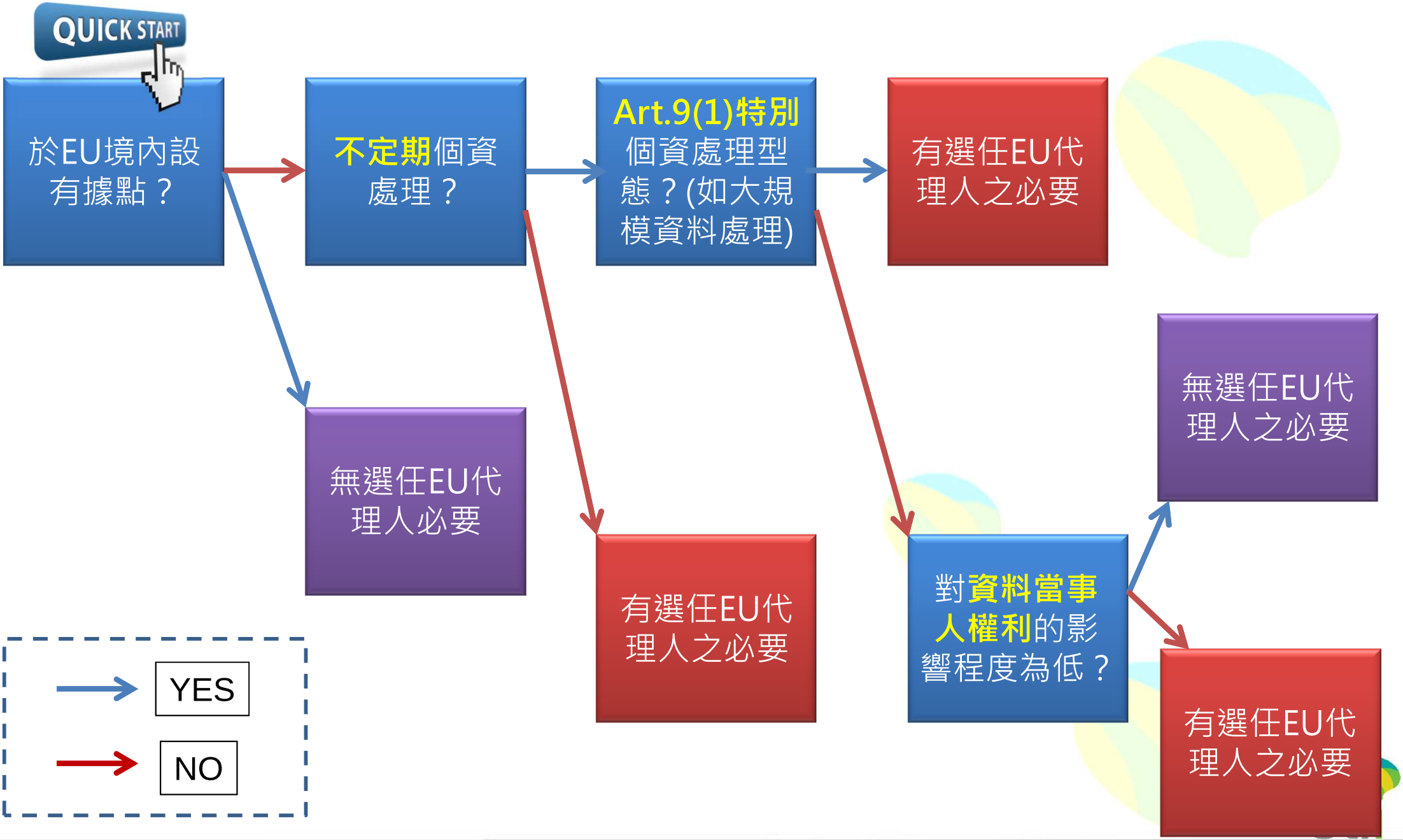
- 客體面：有爭議的資料是不是個資法定義的個人資料？
- 主體面：此時我適不適用個資法？適用那一套標準？
- 行為規範面：是不是合於合法蒐集與利用個資的規定？

■同時了解

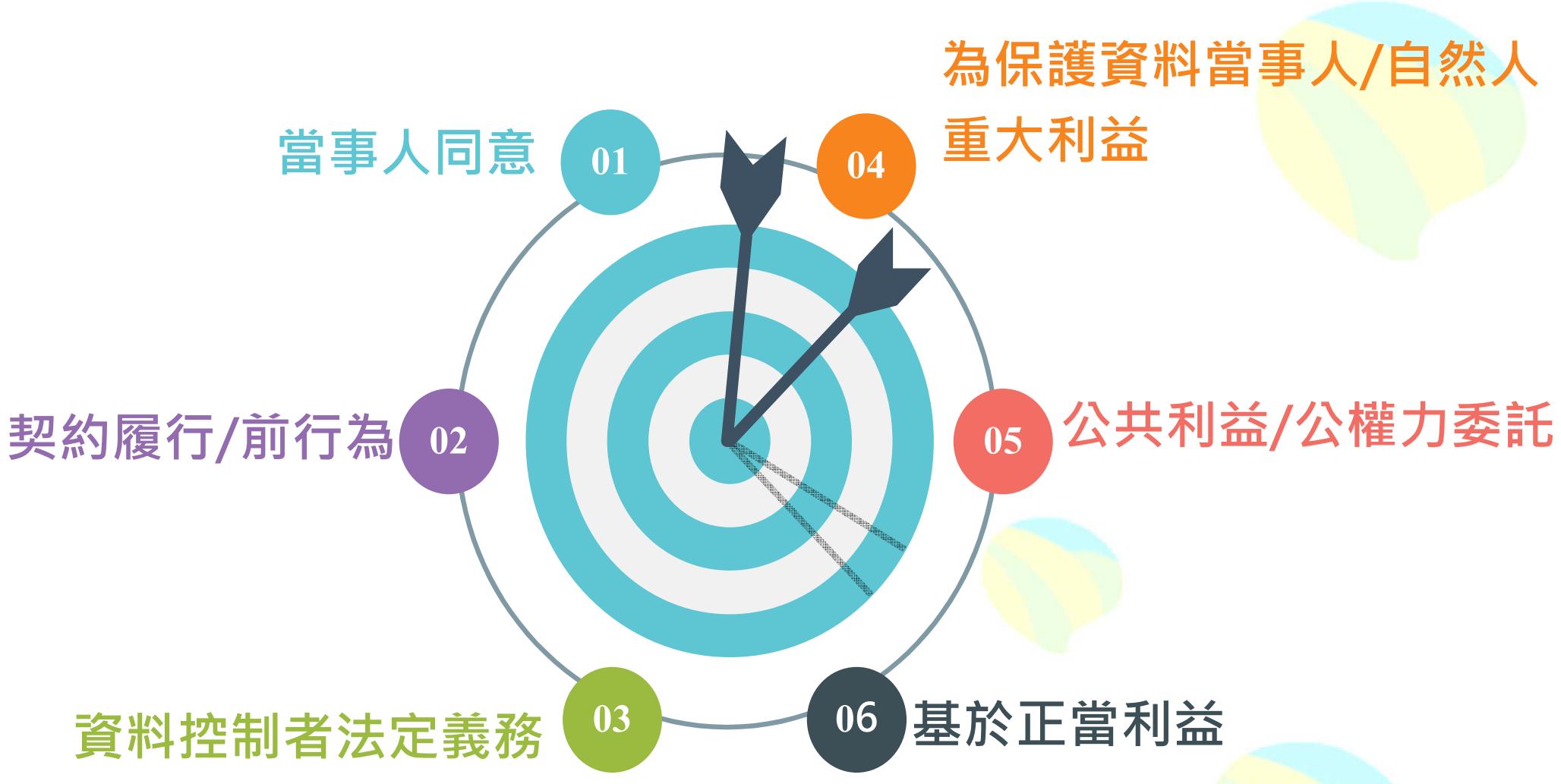
- 當事人面：被我們蒐集資料的人(民眾)可以主張什麼？
- 法律責任面：如何事前降低風險、事後舉證減輕責任

從判斷流程檢視產品、服務是否適用GDPR

歐盟代理人選任評估流程



合法處理個資著眼點



GDPR法遵方式採用考量

標準契約條款（Standard Contractual Clause, SCC）

- 是否訂定，取決於企業意願
- 考量因素：
  - **反映最終承擔風險**：標準契約條款下，損害發生時，因違反第三方受益人條款(third party beneficiary clause)，傳輸方與接受傳輸方負連帶責任
  - **傳輸行為本身具合法性基礎**：適用標準契約條款無須定期檢視(與歐盟-美國隱私盾機制不同)
  - 企業**各自**與歐盟傳輸方**簽締合約**
  - 條款協商需**花費**一定**時間、成本**

具拘束力企業規則(Binding Corporate Rules, BCRs)

- 類似行為準則，由多國企業組成之**團體共同協商**
- 由該團體**統一制定**個人資料國際傳輸的**全球政策**
- 只有依照**經過監督機關許可**的 BCRs，才可在全世界的**企業集團內**合法且自由地進行資料傳輸
- **2014年歐盟企業BCRs與APEC CBPR體系共通參考文件(Common Referential)**：協助企業組織理解與遵守兩種體系要求，對企業個資隱私保護政策與實踐有其實用性

事故因應著眼點

- 識別個人資料事故
- 理解個人資料事故態樣
- 內部管控措施
- 專責人員或專責單位
- 事故評估程序

資料加值應用在GDPR的困境及因應(1/2)

GDPR資料保護意涵	巨量資料分析困境	因應作法
1. **個資處理條件** GDPR要求個資處理應公平合法，且須符合特定情形，如當事人同意等	**難取得同意** 巨量資料分析過程中，取得資料當事人同意可能有實踐困難	**即時告知** 資料當事人同意，可配合即時告知為之
2. **目的限制** 「兩步驟測試」(two-part test)：(1) 蒐集目的應具體且合法；(2) 為公共利益等目的之進階利用，仍應符原蒐集目的	**藉分析探尋新目的** 巨量資料分析具流動、偶發性，藉演算法探詢不在預期範圍內之資料關聯，形成新的資料利用目的。目的限制要求可能造成分析發展障礙	**相容性評估** 尋求不同階段資料處理目的之關聯性：(1)資料當事人合理期待、(2)資料屬性，以及(3)既有安全措施是否足以因應新資料利用目的
3. **資料最小化** 個人資料之蒐集、處理，以及留置期間，應符合資料最小化概念	**影響巨量資料分析效益** 為進行巨量資料分析，資料之蒐集、處理及留置通常會盡可能以最大範圍、期間為之	**建置資訊治理制度** 建議企業定義資料處理目的，以盤點巨量資料分析相關資料。同時，採行良好資訊治理

資料來源：英國「巨量資料、人工智慧、機器學習與資料保護指導文件」，2017年

資料加值應用在GDPR的困境及因應(2/2)

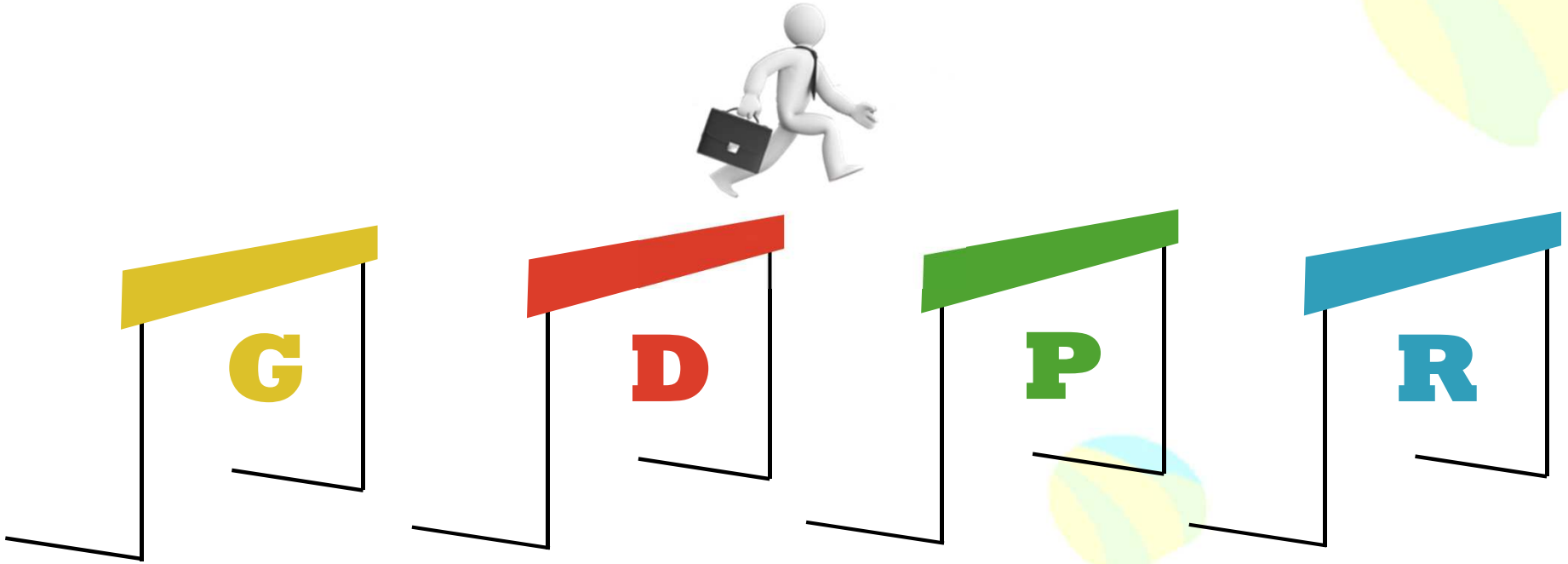
GDPR資料保護意涵	巨量資料分析困境	因應作法
4. 當事人近用權 近用權包括對資料處理、處理目的，以及可能揭露對象之知情權、請求製給複製本權利，以及查詢閱覽權利等	**難以特定當事人** 若係利用非結構性資料等方式分析資料，較難於分析結果上，特定出原資料當事人	**提供近用途徑** 建議參考GDPR前言第63段，由資料控制者提供遠端安全連線，使資料當事人得直接近用其個人資料
5. 安全性 個人資料之蒐集、處理，應採取組織與技術措施，確保安全性	**必存在風險** 巨量資料重複儲存、頻繁委外分析以及不同資料集間的串接，很可能存在違反資料保護規範、資料洩漏等風險	**妥適安全措施** 資料控制者應將前述風險納入風險評估，並據以規劃妥適安全措施
6. 歸責與治理 企業應明確表示其符合GDPR下哪幾項原則，此將對應相應責任	**難釐清實驗性質責任** 紀錄保存目的於巨量資料分析而言，可能存在困難，蓋巨量資料一開始之分析，多為實驗性質、無預設前提，甚至無企業需求	**定期或必要時檢視資訊治理** 建議企業以彈性、變動之資訊治理制度，定期或於必要時檢視因應資料保護規範所要求之回報、內部記錄保存以及資源分配

資料來源：英國「巨量資料、人工智慧、機器學習與資料保護指導文件」，2017年

報告大綱

- 前言
- 歐盟GDPR規範重點與影響
- 企業因應GDPR之作法
- 因應GDPR之相關資源

因應GDPR之相關資源



政府部門指導文件提供法遵方向(1/2)

日本	韓國
個人情報保護委員會(PPC)官網提供GDPR進展、國內影響評估等資訊	個人資訊保護委員會(PPC)2016年提出GDPR分析報告 (EU 개인정보보호법제(GDPR) 분석 및 개인정보보호법제 개선 입법수요 연구)
日本貿易振興機構(JETRO)，提出「EU 一般資料保護規則（GDPR）」相關之實務手冊（入門編）外，另提出5份調查報告供業界遵循參考 1. 2018年2月23日「EU一般データ保護規則（GDPR）」に関わる実務ハンドブック（第29条作業部会ガイドライン編）データ保護責任者（2018年2月） 2. 2018年2月23日「EU一般データ保護規則（GDPR）」に関わる実務ハンドブック（第29条作業部会ガイドライン編）データポータビリティの権利（2018年2月） 3. 2018年2月23日「EU一般データ保護規則（GDPR）」に関わる実務ハンドブック（第29条作業部会ガイドライン編）管理者および処理者の主導監督当局の特定（2018年2月） 4. 2017年8月18日「EU一般データ保護規則（GDPR）」に関わる実務ハンドブック（実践編）（2017年8月） 5. 2016年11月21日「EU一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）(2016年11月）	韓國內政與資訊安全局(KISA)2017年4月提出指導文件(Guidance on “General Data Protection Regulation” for Korean Enterprises)提供該國企業遵循參考

政府部門指導文件提供法遵方向(2/2)

- ◆國家發展委員會個人資料保護專案辦公室
  - ➢設立GDPR網站專區
  - ➢歐盟GDPR之相關部會諮詢窗口
- ◆澳洲資訊委員辦公室（OAIC）：
  - ➢ **Australian businesses and the EU General Data Protection Regulation**
- ◆香港個人資料隱私專員公署：
  - ➢提供中英文版本「歐洲聯盟通用數據保障手冊2016」

國家發展委員會 NATIONAL DEVELOPMENT COUNCIL

Australian Government
Office of the Australian Information Commissioner

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

協助企業因應GDPR調適舉措(1/2)

◆英國資訊委員辦公室（ICO）：

➢ICO每月公布GDPR相關法遵文件與技術指引：例如8月公布國際傳輸指南，7月公布自動化決策指南、隱私設計及預設指南、資料保護影響評估指南等

➢提供資料保護自我評量線上工具（ Data protection self assessment）：

✓提供各種依GDPR法規主體角色不同的檢核表，例如控管者、處理者。

✓以及不同功能的檢核表，例如直接行銷、資料分享與資料主體接取、CCTV等

協助企業因應GDPR調適舉措(2/2)

- ◆European Union Agency for Fundamental Rights and Council of Europe
  - ➢ Handbook on European data protection law 2018 edition
- ◆Taylorwessing
  - ➢ GDPR Audit Checklist
- ◆ecommerceguide.com
  - ➢GDPR: A Guide for Ecommerce
- ◆Cloud Industry Forum
  - ➢ The Cloud and the EU GDPR: Six Steps to Compliance

TaylorWessing

CLOUD INDUSTRY FORUM

Ecommerce Guide

推動資料治理與資料共享

- 資料跨域應用已逐漸為各國所重視，藉由分析大數據，可以開拓資料經濟，進而創造產品創新價值並培育新興市場，提供企業未來競爭優勢及可持續性成長、發展
- 藉由「政策透明」、「隱私設計」等措施，甚至中長期修立法，輔以隱私設計技術，將可提升資料當事人之信賴，促進資料之流通與加值應用，實現資料經濟

經濟部因應GDPR施行之策略與作法

經濟部

107月9月14日

大綱

壹 GDPR施行之影響評估

貳 經濟部因應GDPR施行之策略

參 經濟部因應GDPR施行之作法

壹、GDPR施行之影響評估

一、調查產業受GDPR施行之影響

透過向個別廠商**面訪**、**電訪**與**問卷調查**、**座談會**等方式，進行瞭解本局所業管產業因應GDPR所採之措施(包括所遇困難與期獲得協助之事項)，作為**研擬協助**企業因應GDPR之參考。

二、GDPR施行對我國企業之影響與衝擊分析

企業情形		影響	衝擊
1.於歐盟境內設有據點者		直接且立即	中
2.未於歐盟境內設立據點者	2-1. 受歐盟企業之委託進行個人資料之蒐集、處理與利用	間接	小
	2-2. 對歐盟境內居民提供商品/服務或監控其行為，且有蒐集個人資料	直接且立即	大
	2-3. 銷售產品或提供服務至歐盟境內，但不涉及個人資料之蒐集、處理或利用	無	無
	2-4. 無歐洲業務	無	無

三、GDPR施行對電子資訊業之影響與衝擊

GDPR之施行對金屬機電、民生化工、環境永續產業、資訊服務產業影響不大或暫無影響，而電子資訊業因為業者**行為態樣較多元**且**有跨國企業、全球品牌業者、網路應用**者等，故GDPR之施行對該產業有一定程度之影響，但大型業者多已經或著手因應GDPR之施行。

影響	電子資訊業之行為態樣
直接立即	● **於歐盟境內設立代工廠、子公司等據點者或大型品牌商**(對歐盟消費者銷售產品)，為GDPR實施之直接衝擊對象。 ● 因雲端服務、APP服務等**網路應用服務**，而有大量蒐集、處理或利用歐洲境內人民之個人資料。。
間接	● 作為歐洲企業之資料處理者。 ● 以B2B為商業模式，受客戶要求須符合GDPR。
無	● 以系統設備、晶片為主，認無涉及個人資料。 ● 非跨國企業、無歐盟設立公司且無歐盟業務。 ● 有歐盟業務，但無涉歐盟居民資料之蒐集，尤其是B2B為主者。

貳、經濟部因應GDPR施行之策略

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

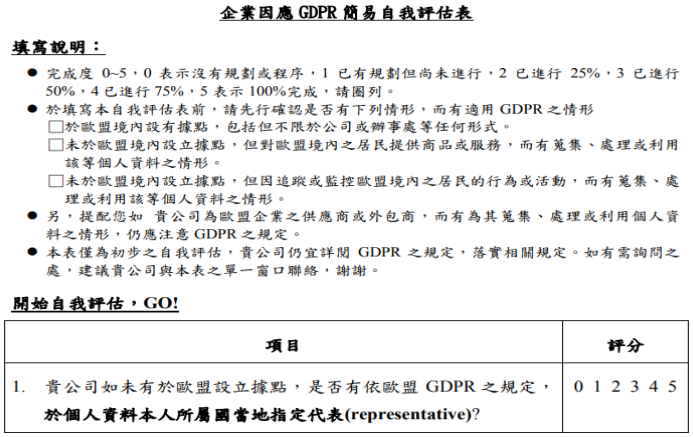
- 透過新興資安產業生態系推動計畫網站(https://www.acw.org.tw/)，**提供法規、實作、標準、顧問與解決方案提供者資訊、評估小工具等**

[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



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，提配您如 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

- **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

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

優先順序	受測產業
■ 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	■ 資通訊製造業 ■ 雲端物聯網產業 ■ 金融服務產業 ■ 中小企業

建立檢測診斷流程

風險評估	資安檢測
■ 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)	■ 網路封包側錄分析 ■ 弱點掃描檢測 ■ 資訊設備組態基準檢測

建立診斷驗收機制

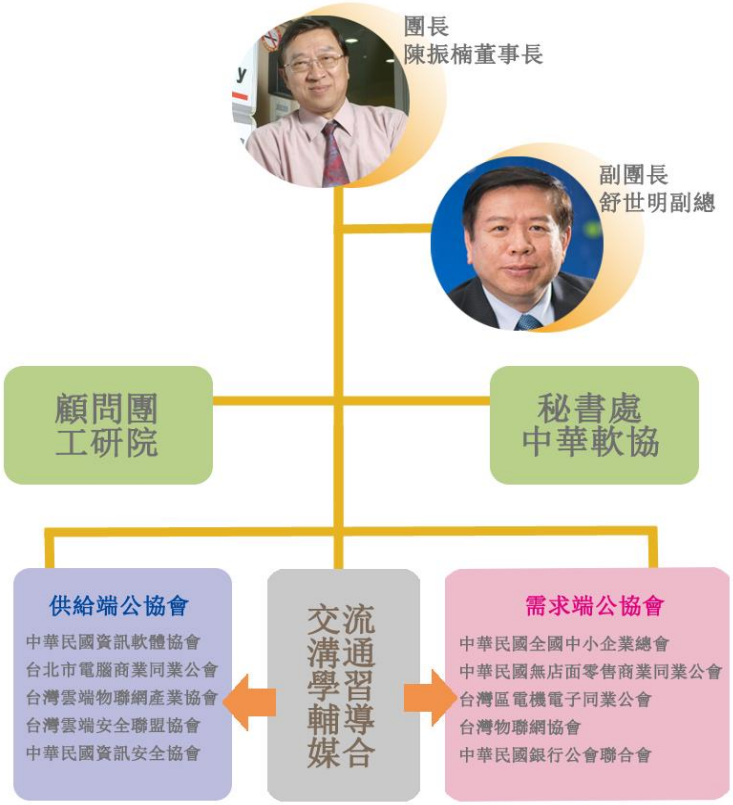
顧問服務報告
■ 資訊安全風險現況評估報告 ■ 資訊安全技術檢測報告 ■ 資訊安全風險控制建議報告

附件

- 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

簡報結束，謝謝聆聽！

金融業因應歐盟一般資料保護規則(GDPR)施行之相關作為

金融監督管理委員會報告

107年9月14日

大 綱

一、我國金融業於歐盟地區設立情形及相關處置

二、我國金融業具體因應措施-以銀行業為例

三、金管會因應GDPR之具體協助措施

我國金融業於歐盟地區設立情形及相關處置

銀行業

- **6家本國銀行：於歐盟境內設立7分行及1子行**
- 歐盟當地分行或子行處理歐盟自然人個資流程必須完整遵循GDPR及當地相關法規規定，而我國銀行總行就取得之歐盟自然人資料相關處理運用方式應遵循歐盟GDPR規定。
- 於歐盟當地設有據點之6家本國銀行，已採取適當措施。

我國金融業於歐盟地區設立情形及相關處置(續)

證券業

- **2家證券公司：於歐盟境內設立2家子公司**
- 上開歐盟子公司之營運模式均係**轉介客戶至其他海外子公司開戶，且以法人戶為主**，原則不碰觸客戶個資，保有歐盟居民個資均為員工個資。

我國金融業於歐盟地區設立情形及相關處置(續)

壽險業

- **2家保險公司：於歐盟境內設立8家特殊目的公司（SPV公司）**
- 上開公司均**非從事保險業務**。該等公司除少數員工個資外，尚未涉及蒐集當地居民個資，經上開公司洽請顧問評估認為該等公司於歐盟地區設立之子公司不適用GDPR規定。

我國金融業具體因應措施-以銀行業為例

一、於歐盟當地有分支機構之銀行業

進行個資盤點

包括歐盟個資人數、業務範圍及是否適用GDPR之評估。

強化隱私資料之保護

1. 配合GDPR進行內部作業規範調整
2. 檢視網路資安防護系統
3. 建置個資外洩時之通報機制

GDPR規範之比較

1. 完成法規差異分析
2. 評估建置個人資料可攜權、被遺忘權、限制權之機制。
3. 禁止犯罪前科資料之處理。

資料處理程序之調整

1. 檢視隱私資料蒐集、處理與利用的要件，包含：清楚、積極之同意、法定蒐集要件，配合調整相關契約條款。
2. 委託/諮詢外部顧問/律師提供專業協助處理，並依GDPR原則簽署同意遵循當地資料保護規範。

跨境傳輸之因應

因應GDPR跨境傳輸原則簽署SCC (Standard Contractual Clauses)或申請BCRs(Binding Corporate Rules)

設置資料保護長

4家已設置，1家不設置，1家不設置DPO但於倫敦設置聯絡窗口（DPR）。

我國金融業具體因應措施-以銀行業為例(續)

二、於歐盟當地未有分支機構之銀行業

若其業務涉及對歐盟境內自然人提供商品或服務，或對歐盟境內自然人所為之監控，仍應適用GDPR規範

◆ 由總行或委託相關顧問公司協助進行差異性分析及影響範圍，並就個資蒐集、處理程序及個資當事人權利告知等事項，研議修正銀行個資同意書範本等相關規章。

◆取得歐盟自然人個資之銀行均已辦理法規差異分析，並已完成網路資安防護措施之檢視，及參加銀行公會及聯徵中心舉辦之相關宣導活動，並辦理內部教育訓練。

◆取得歐盟自然人個資較少之銀行，依據銀行公會推估，該等銀行被歐盟認為「有意圖為歐盟境內之自然人提供商品或服務」而適用歐盟GDPR之可能性甚低。

金管會因應GDPR之具體協助措施

於GDPR施行前，金管會已先請金融聯合徵信中心與銀行公會報告瞭解國內金融業者可能產生之影響、風險及後續之因應作法，並請該二單位於107年5月17日共同舉辦「金融業因應歐盟個人資料保護規則」研討會，藉此提供金融同業交流分享因應GDPR相關知識及經驗之機會。

督導銀行公會建置所屬會員公司適用歐盟GDPR規範資訊交流平臺，及透過洽詢歐盟當地顧問律師專業意見、彙整會員公司適用GDPR規範經驗分享、擬定個資保護檢視調整清單、指引及具體明確之因應措施方案，提供所屬會員遵循歐盟GDPR規範之參考。

督導證券期貨公會及保險公會協助所屬會員公司比照銀行公會之方式，以確保所屬業者落實GDPR之法令遵循。

金管會因應GDPR之具體協助措施(續)

協助金融業者對於GDPR規範之適用疑義，可由公會蒐集彙整報送本會轉請經濟部駐歐盟經濟組協助洽詢歐盟GDPR主管機關司法總署（DG JUST）釐清。

GDPR的國際資料傳輸係採取「原則禁止、例外開放」，如欲傳輸個人資料到第三國，其中例外開放方法之一為確保第三國個資保護程度已符合GDPR標準而取得適足性認定，即第三國須通過歐盟執委會的適足性評估程序，目前我國與歐盟洽談跨境傳輸適足性認定之主政單位，由國家發展委員會擔任，本會配合提供資料以利國發會辦理向歐盟申請適足性認定之作業事宜，包括提供（1）適足性指引揭示之評估要項及相關法規（2）金融業者落實GDPR實質內容在我國執行上疑義

持續注意歐盟GDPR施行之相關細則或指引之公布，及歐盟各會員國監管機關之執行及解釋上的差異，督導金融業者符合歐盟GDPR規範之要求。

感謝聆聽
敬請指教

中華民國交通部

歐盟一般資料保護規則(GDPR)北中南宣導說明會

-交通部面對GDPR之相關因應措施

交通部

107年9月14日

簡報大綱

一、個人資料保護法之辦理情形

二、因應GDPR之辦理情形

三、結語

一、個人資料保護法之辦理情形(1/3)

- **依據個人資料保護法第18條規定，公務機關應指定專人辦理安全維護事項；同法施行細則第12條規定所稱之適當安全維護措施包含「認知宣導及教育訓練」，本部自101年起每年定期舉辦教育宣導講習。**

- **本部依據個人資料保護法訂定相關要點如下：**

(一)99年11月30日訂定發布「交通部個人資料保護管理要點」。

(二)101年10月30日訂定發布「交通部個人資料檔案安全維護計畫」。

二、個人資料保護法之辦理情形(2/3)

- **本部依據個人資料保護法訂定相關配套子法如下：**

(一)103年1月3日訂定發布「觀光旅館業個人資料檔案安全維護計畫辦法」；並自103年4月1日施行。(觀光局)

(二)103年10月16日訂定發布「民用航空運輸業個人資料檔案安全維護計畫及處理辦法」；並自104年1月1日施行。(民用航空局)

(三)104年4月17日訂定發布「船舶運送業個人資料檔案安全維護計畫及處理辦法」；並自104年7月1日施行。(航港局)

(四)104年5月5日訂定發布「旅行業個人資料檔案安全維護計畫及處理辦法」；並自即日施行。(觀光局)

(五)104年9月24日訂定發布「停車場經營業個人資料檔案安全維護計畫及處理辦法」；並自105年1月1日施行。(路政司)

(六)104年12月23日訂定發布「觀光遊樂業個人資料檔案安全維護計畫辦法」；並自即日施行。(觀光局)

- **本部各所屬機關均已訂定個人資料安全維護相關規定，公務個人資料檔案，皆有專人保管維護。**

一、個人資料保護法之辦理情形(3/3)

基礎關係（法律要件/四字箴言）

目的 ＋ 必要

蒐集
以任何方式取得個人資料

處理
為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、 編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送

利用
將蒐集之個人資料為處理以外使用

個人資料

二、因應GDPR之辦理情形(1/16)

(一)除以上本部所訂定之6個相關「個人資料檔案安全維護計畫及處理辦法」已可符合GDPR相關規定(如下說明)外，本部已於107年5月7日邀請達文西科技法律事務所所長葉奇鑫律師向本部暨所屬機關(構)講授GDPR相關事宜。

(二)歐盟適足性要項評估比對(1/3)

二、因應GDPR之辦理情形(2/16)

(二)歐盟適足性要項評估比對(2/3)

特種個資之保護

自動決策及剖析

拒絕行銷權

貳、其他特殊處理原則例示

參、程序與執行機制

肆、基於執法和國家安全對基本權利干預之限制

主要涉及我國個人資料保護法整體執行面及我國法制環境，交通部配合辦理。

二、因應GDPR之辦理情形(3/16)

(二)歐盟適足性要項評估比對(3/3)

(適足性要項)	(處理辦法)
壹、個資保護應具備之核心原則	交通部所訂定之6個「個人資料檔案安全維護計畫及處理辦法」，**符合**歐盟適足性評估基本要項。
貳、其他特殊處理原則例示	
參、程序與執行機制	未來依我國個資法與GDPR相關規定**調整後銜接**，並配合行政院、國發會指示辦理。
肆、基於執法和國家安全對基本權利干預之限制	

綜整比對

本部主管業務龐雜，以下謹就GDPR與本部主管業務較相關之民航、航港及觀光部分說明辦理情形。

二、因應GDPR之辦理情形(4/16)

(三)民航之國籍航空辦理情形(華航)

GDPR 對企業關鍵影響層面

法遵層面	資訊技術層面	資料層面
■ 當責 Accountability	■ 資料外洩通知 Breach notification	■ 個資清單Data inventories
■ 隱私聲明與同意 Privacy notice and consent	■ 資料加密 Encryption	■ 新個資定義New definitions of data
■ 行政罰款 Enforcement Fines	■ 線上分析Online profiling	■ 被遺忘權Right to be forgotten
■ 資料保護長 DPO(Data Protection Officer)	■ 預設保護隱私設計 Privacy by design and by default	■ 資料可攜權Right to data portability

二、因應GDPR之辦理情形(5/16)

(三)民航之國籍航空辦理情形(華航)

華航GDPR專案與時程---於2018年初引進顧問「**勤業眾信Deloitte**」專案團隊協助，確認專案計劃項目及時程如下：

- 第一階段-**隱私保護現況評估**：01/18~02/14
  Evaluate existing status of privacy protection.
- 第二階段-**差異分析與改善規劃**：02/21~04/02
  Gap analysis and improvement plan.
- 第三階段-**設計與建置隱私保護計畫**：04/03~05/10
  Design and implement privacy protection action plan items
- 第四階段-**隱私保護計畫運行與改善**：05/11~05/28
  Execute privacy protection action plan and improve accordingly.

二、因應GDPR之辦理情形(6/16)

(三)民航之國籍航空辦理情形(華航)

- 辦理多場OJT訓練，超過千名員工參與，其中包含華信、虎航、各外站經理會議、客艙經理複訓。
- 3月26日於EIP公告GDPR相關注意事項，3月29日進行e-Learning全體員工線上教育訓練。
- 進行11個單位個資盤點，產出181個BIF檔案(Business Information Framework)。
- 107份相關文件修訂(SOP x 56, 手冊 x 4, 表單 x 47)。
- 修訂資料隱私與安全政策。
- 建立個資事件管理平台PDEHP(Personal Data Event Handling Platform)。
- 與第三方供應商加簽SCC附約(標準個資保護契約條款，Standard Contractual Clauses)。
- 會員網站增加同意選項Dynasty Member opt-in consent。

二、因應GDPR之辦理情形(7/16)

(三)民航之國籍航空辦理情形(長榮)

專案策略

- 長榮現於歐盟地區有5家分公司，分別於倫敦、阿姆斯特丹，巴黎、法蘭克福及維也納提供旅客訂位與搭機服務，依資料處理量、跨境傳輸等條件判斷應屬GDPR管轄範圍。
- 因應GDPR以及未來國際個資保護趨勢，同時參考盟航推行經驗，檢視並強化公司現有資安及個資保護制度。
- 由公司資訊安全委員會主導，以專案方式成立工作小組進行GDPR合規相關事宜。
- 因應GDPR之法遵規定及實際作業面與系統面之合規確認，引進熟稔歐盟法務及法遵實務之外部顧問公司，以其專業知識與方法以及實際專案執行經驗，協助本案進行以強化時效。

二、因應GDPR之辦理情形(8/16)

(三)民航之國籍航空辦理情形(長榮)

執行規劃(1/3)

- 本專案規劃於程序、法規、系統及宣導等相關面向進行調整與強化，茲將專案項目條列如表列：

類別	作業項目
程序面	● 強化當事人權利行使程序與管道 ● 執行隱私資料辨識與盤點作業 ● 規劃隱私衝擊分析機制(DPIA) ● 規劃預設隱私保護流程(PbD) ● 修訂供應商個資處理安全管理機制 ● 修訂事件通報應變機制 ● 執行隱私保護計劃實施有效性評估

二、因應GDPR之辦理情形(9/16)

(三)民航之國籍航空辦理情形(長榮)

執行規劃(2/3)

類別	作業項目
法規面	● 供應商合約盤點與修訂 ● DPO因應措施規劃 ● 資料保存期限策略規劃 ● 當事人權利各類公告及表單檢視與修訂 ● 調整隱私保護組織與權責 ● 強化個資跨境傳輸規則(以拘束性企業規則BCR方式)
系統面	● 旅客接觸管道之當事人權益相關修改 ● 檢視並調整電子行銷系統(EDM) ● 以個資最小化原則檢視並縮減個資傳輸內容 ● 評估資訊科技環境隱私保護風險 ● 強化數位證據封存與保全機制

二、因應GDPR之辦理情形(10/16)

(三)民航之國籍航空辦理情形(長榮)

執行規劃(3/3)

類別	作業項目
宣導面	● GDPR認知教育訓練(e-Learning) ● 個資識別與隱私清冊應用說明

- **本專案已完成基本合規建置，包括程序面、法規面、系統面及宣導面等相關作業。**

二、因應GDPR之辦理情形(11/16)

(四)航港辦理情形

- 台北市海運承攬運送商業同業公會於107年7月19日主辦歐盟個人資料保護規範研討會

主講者:標竿企業BSIGroup英國標準協會台灣分公司總經理蒲樹盛

- 出席交通部辦理之年度「個人資料保護法講習」

- 設立專責窗口

- 年底邀請講師舉辦宣導會

二、因應GDPR之辦理情形(12/16)

(五)觀光辦理情形

旅行業現況

- 可辦理境外業務之綜合及甲種旅行業，總公司及分公司數量計3,628家(107年8月)。
- 目前尚無旅行社在歐盟地區登記設立公司(107年8月)。
- 國內法部分，旅行業個資保護依據為「個人資料保護法」及「旅行業個人資料檔案安全維護計畫及處理辦法」(104年5月5日交路（一）字第10482001664號令訂定發布)。

二、因應GDPR之辦理情形(13/16)

(五)觀光辦理情形

觀光旅館業現況

- 觀光旅館業家數總計127家，其中國際觀光旅館計79家，一般觀光旅館計48家(107年8月)。
- 國內除晶華、雲朗的關係企業有在歐盟地區設立營業據點，其餘均無。
- 國內法部分，觀光旅館業個資保護之依據為「個人資料保護法」及「觀光旅館業個人資料檔案安全維護計畫辦法」(103年1月3日交路（一）字第10282007761號令訂定發布)。

二、因應GDPR之辦理情形(14/16)

(五)觀光辦理情形

是否有GDPR的適用？

- 是GDPR規範之義務人
  1、在歐盟地區登記設立公司者
  2、直接向歐盟地區旅客收集個資
  3、雇用歐盟地區員工
- 非GDPR規範之義務人
  1、非上述情形
  2、間接透過在歐盟地區登記設立公司的Booking.com取得歐盟旅客個資

二、因應GDPR之辦理情形(15/16)

(五)觀光辦理情形

個資防護作為

- 觀光局已分別於107年3月26日及4月25日函請各旅行業、觀光旅館業及旅館業公會確實向各所屬會員宣導個資防護及轉知GDPR資訊。
- 辦理觀光旅館業定期或不定期查核，督導業者落實執行「個人資料檔案安全維護計畫」及防範個資外洩，105年查核計77家次，106年查核計58家次。
- 辦理旅宿業中階經理人訓練課程，納入個人資料保護法相關規定加強宣導，105年宣導401人次，106年宣導396人次。
- 除針對各旅行社進行定期之業務檢查，督促各旅行業者防範個資外洩。觀光局已設置稽查小組，每月皆有安排查核，不特定抽檢各旅行業者，查核其業務經營情形，如有特定疑似違法旅行業者(如受民眾檢舉、其他機關之移送或辦理因執行職務而發現之舉發情形)則優先排查。
- 已於全臺辦理8個場次資訊安全說明會，對業者進行個資防範說明，以落實各旅行業者個資維護計畫。

二、因應GDPR之辦理情形(16/16)

(五)觀光辦理情形

交通部觀光局個資保護與GDPR行政差異

交通部觀光局	GDPR
■ 未設獨立專職組織 ■ 企業未強制設立個資長 ■ 未依規定蒐集、處理或利用個資，依違反情形可處新臺幣2萬元以上20萬元以下(個資法第48條)、或新臺幣5萬元以上50萬元以下(個資法第47條)罰鍰	■ 應設立獨立組織 ■ 依GDPR第37條規定達一定要件應設個資長 ■ 未依規定處理個資，依違反情形可處1千萬歐元或全球年營業額2%罰鍰；或2千萬歐元或全球年營業額4%罰鍰

三、結語

- 數位經濟時代，資料就是貨幣。

- GDPR強化個資保護，平衡當事人權利與企業利益，藉以增加對數位服務之信任，長期應有促進經濟發展之效果。

- 藉由主動積極推動企業符合GDPR規範之作為，落實當責，以強化企業(公司)競爭優勢，提升品牌信賴感，讓潛在之財務風險極小化。

感謝聆聽，
敬請指教！

通傳會因應GDPR之作為分享

國家通訊傳播委員會

107年9月14日

大　　綱

一、前言

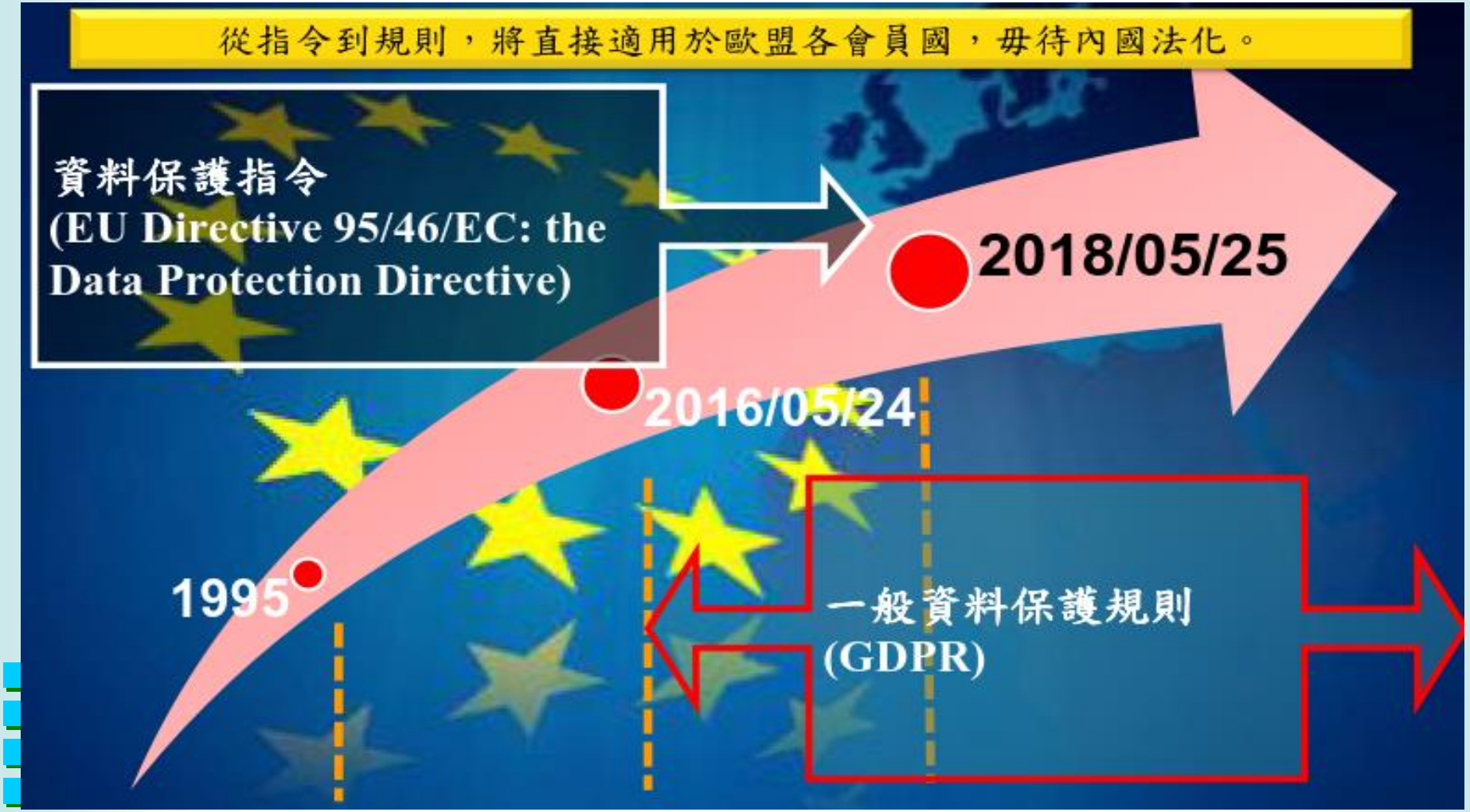
二、個資保護法遵要項概覽

三、通傳會因應GDPR作為分享

四、結論

前言

- **GDPR: 執法進程**


從指令到規則，將直接適用於歐盟各會員國，毋待內國法化。
資料保護指令
(EU Directive 95/46/EC: the Data Protection Directive)
2018/05/25
2016/05/24
1995
一般資料保護規則
(GDPR)

個資保護法遵要項概覽（法律架構）

個人資料保護法

其他特別法

個人資料保護法施行細則

個人資料檔案安全維護計畫及業務終止後個人資料處理方法之辦法

目前計有中央銀行、內政部、公平交易委員會、交通部、行政院公共工程委員會、行政院原子能委員會、行政院農業委員會、金融監督管理委員會、財政部、教育部、勞動部、**經濟部**、**國家通訊傳播委員會**等13部會針對其所轄非公務機關，發布相關辦法。

105.11.9

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法

個資保護法遵要項概覽（檔案安全維護）

個資法第27條

- 非公務機關應採行適當安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏

主管機關得要求非公務機關訂定

- 個人資料檔案安全維護計畫
- 業務終止後個人資料處理方法

施行細則第12條

- 明確界定指「組織上」及「技術上」之措施
- 提出11款個資檔案安全維護措施包括之事項

授權中央目的事業主管機關訂定

- 個人資料檔案安全維護計畫辦法
- 業務終止後個人資料處理方法辦法

個資保護法遵要項概覽(適當安全維護措施)

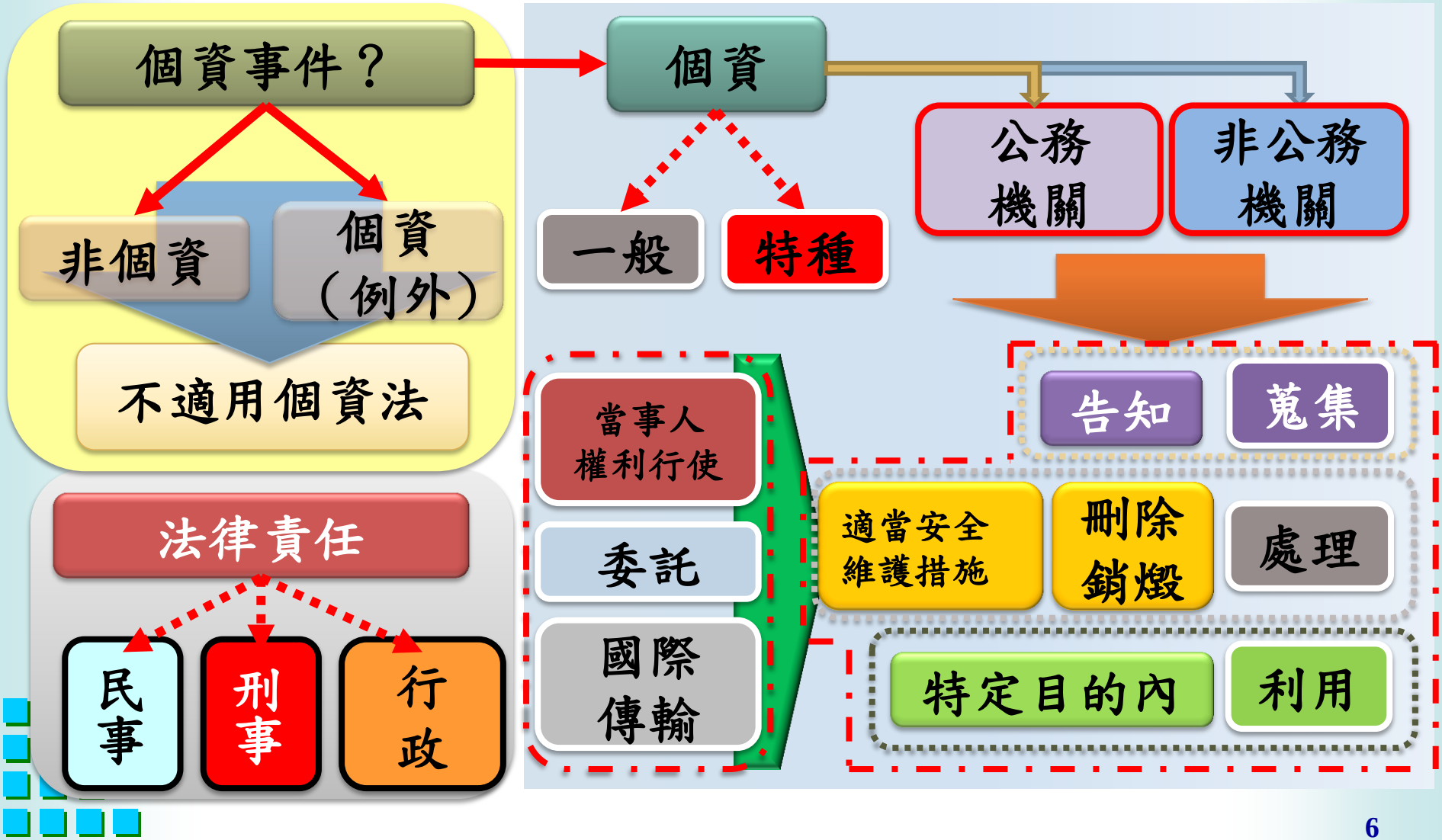
個人資料保護法施行細則第12條II

◆適當安全維護措施、安全維護事項、適當之安全措施

＝符合比例原則之

1.配置管理之人員及相當資源
2.界定個人資料之範圍（個資盤點）
3.個人資料之風險評估及管理機制（風險評鑑）
4.事故之預防、通報及應變機制
5.個人資料蒐集、處理及利用之內部管理程序。
6.資料安全管理及人員管理
7.認知宣導及教育訓練
8.設備安全管理
9.資料安全稽核機制
10.使用紀錄、軌跡資料及證據保存
11.個人資料安全維護之整體持續改善

個資法遵要項概覽(個資全生命週期流程圖)



通傳會因應GDPR作為分享辦理情形(1/2)

106.3	內部成立『資料運用及隱私保護規範政策工作小組』
106.3~10	依前開工作小組會議，由通傳會業管處依指定非公務機關個人資料檔案安全維護辦法擬定通傳事業個資維護執行情形自評表，並分別發函第一、二類電信業者、有線電視業者、無線廣播、無線電視、衛星廣播電視業者(含新聞頻道、購物頻道、他類頻道及直播衛星業者)進行調查，調查合計805家
106.7~107.1	辦理「通訊傳播產業資料加值與創新應用趨勢及法令研析」委託研究案(公布本會官網首頁>政府資訊公開>研究及出國報告>委託研究計畫)
106.10	邀集五大電信事業及五大MSO業者召開「研商資料運用及隱私保護相關議題會議」以先行瞭解業者執行情形。

通傳會因應GDPR作為分享辦理情形(1/2)

106.11～107.3	函發「第一類電信事業辦理個人資料檔案安全維護執行情形查訪計畫」及「有線電視系統經營者辦理個人資料檔案安全維護執行情形查訪計畫」分別前往15家指標性業者辦理實地查訪作業
107.3	辦理「107年度通訊傳播事業導入資料加值應用及隱私保護機制」計畫補助案
107.5~6	依前開計畫針對會內同仁及通傳事業辦理「個人資料保護與管理教育訓練講座」及「通訊傳播事業個資保護與管理教育訓練講座」
107.3~7	依前開計畫辦理「個人資料保護與管理法遵參考文件及個人資料保護與管理適法性稽核檢查作業參考文件」專家座談會及業者說明會，並公布本會官網首頁>新聞公告>熱門議題>隱私保護機制專區）

通傳會因應GDPR作為分享
盤點通傳業者之需求

GDPR影響之議題	業者希望通傳會協助作為
GDPR之認知	舉辦及宣導個資法及GDPR、CBPR等隱私保護政策之教育訓練及研討會
管理制度建置（風險管控）GDPR §32	協助建置管理範本、提供諮詢輔導服務的管道及遵法參考指引；辦理遵法行政稽核作業，協助業者完善個資維護機制
境外傳輸 RECITALS 107；§45	歐盟採取「原則禁止、例外開放」作法，欲傳輸個人資料至第三國，須確保第三國已達到「適當之保護水平」，始得傳輸之。
特定目的利用（同意權§7、被遺忘權§17）	督促業者完善定型化服務契約內容，針對特定目的利用範圍之明確性
救濟準備	研擬國際通傳事業數位市場策略之規範、實例及因應；法遵文件；法制諮詢小組

通傳會因應GDPR作為分享

「107年度通訊傳播事業導入資料加值應用及隱私保護機制」計畫補助案(1/6)

- 於107.1.10經本會第783次委員會議決議，辦理「數位匯流/IoT資安威脅防禦機制暨資安實驗室建置與服務」案之分項五「建構數位匯流/IoT隱私保護機制」子項：

5.1研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制

- 針對 e-Privacy 檢視並研析規範之需要
- 舉辦業界訪談及研討會
- 法制諮詢服務小組

5.2規劃通訊傳播事業導入資料加值應用及隱私保護機制計畫

- 供通傳會及業者相關隱私保護教育訓練資源
- 提供法遵文件完善風險管理
- 辦理查核作業及報告作為政策規劃依據

通傳會因應GDPR作為分享

「107年度通訊傳播事業導入資料加值應用及隱私保護機制」計畫補助案(2/6)

- 活動照片紀實

【通傳會個人資料保護與管理教育訓練講座】
05.23 &06.08

通傳會因應GDPR作為分享

「107年度通訊傳播事業導入資料加值應用及隱私保護機制」計畫補助案(3/6)

【通傳事業教育訓練講座】

05.29台北場一

05.31台中場 .

06.01高雄場 .

06.11台北場二

- 活動照片紀實

通傳會因應GDPR作為分享

「107年度通訊傳播事業導入資料加值應用及隱私保護機制」計畫補助案(4/6)

- 法遵文件座談會紀實
  107.05.09上午

參與座談會學者專家	
華梵大學資訊管理學系	朱惠中教授
SGS台灣檢驗科技股份有限公司	何星翰經理
SGS台灣檢驗科技股份有限公司	柯富聰經理
Afnor法國・貝爾國際驗證機構法國標準集團	杜貴忠主任稽核員
台灣電信產業發展協會	劉莉秋副秘書長
台灣通訊學會	許也翔先生
中華民國衛星廣播電視事業商業同業公會	陳依玫秘書長
台灣有線寬頻產業協會(CBIT)	曾麒霖處長
中華民國電視學會	洪貴淑小姐

通傳會因應GDPR作為分享

「107年度通訊傳播事業導入資料加值應用及隱私保護機制」計畫補助案(5/6)

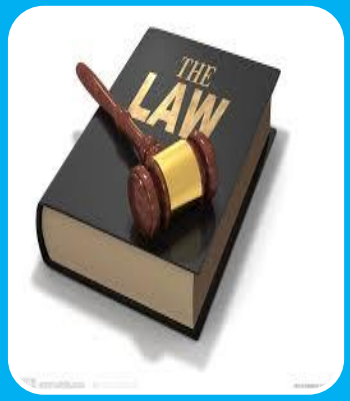
- 稽核檢查文件座談會紀實　107.5.9 下午

參與座談會學者專家	
中華民國品質學會	張文昌主任委員
SGS台灣檢驗科技股份有限公司	何星翰經理
SGS台灣檢驗科技股份有限公司	柯富聰經理
台灣電信產業發展協會	劉莉秋副秘書長
台灣通訊學會	許也翔先生
中華民國衛星廣播電視事業商業同業公會	陳依玫秘書長
輔仁大學法律學院財經法律學系	翁清坤助理教授
台灣有線寬頻產業協會(CBIT)	曾麒霖處長

通傳會因應GDPR作為分享

「107年度通訊傳播事業導入資料加值應用及隱私保護機制」計畫補助案(6/6)

通傳會因應GDPR作為分享通傳網路資安策略之現況(1/2)



完備資安法規環境(各事業業務管理規則增訂「資通安全管理」專章)

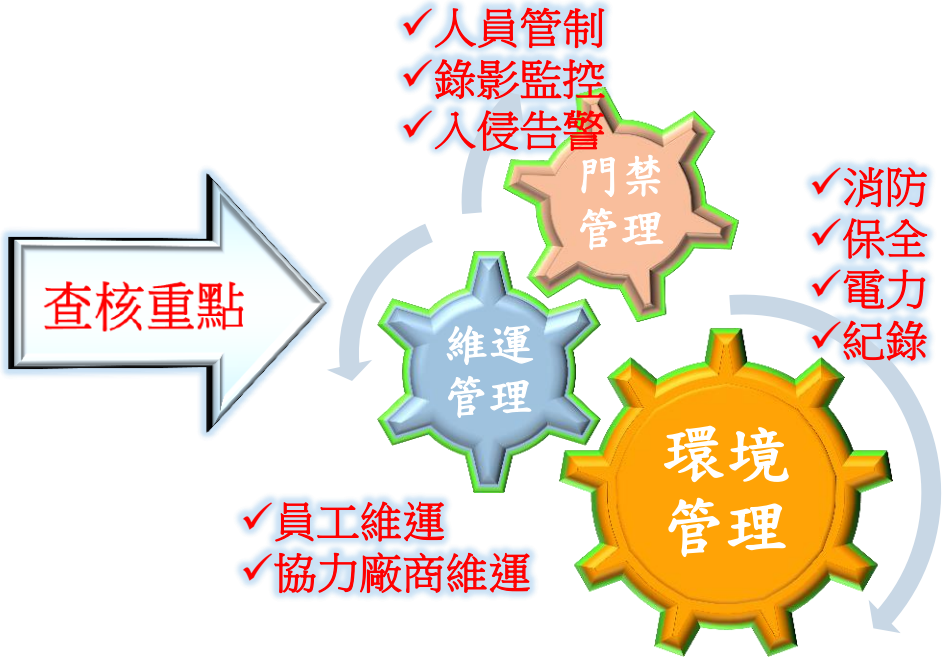
- 建置資通安全防護與偵測設施
- 資通安全事件通報、處理、回報
- 通過CNS(ISO/IEC) 27001及ISO/IEC 27011稽核驗證

強化網路安全管理

- 通傳會業向行政院資通安全處提出106~109年之4年期「數位匯流/IoT資安威脅防禦機制暨資安實驗室建置與服務計畫」，將建置「通訊傳播網路資通安全防護中心」

通傳會因應GDPR作為分享通傳網路資安策略之現況(1/2)

➢ 提升業者防護能力



通傳會因應GDPR作為分享後續辦理規劃

持續辦理107年度行動寬頻事業電信機房安全行政檢查實施計畫(107.4~11)

預計於9月中旬舉辦通傳資料加值應用之法制展望研討會

預計於10月份起就指標性20家通傳事業進行個資保護與管理制度實地查核作業

結論

隱私意識

謹慎選商

資源提供

保護責任

監督管理

優質業者

19

簡　報　完　畢

敬　請　指　教