歐盟「一般資料保護規則」（General Data Protection Regulation, GDPR）簡介與政府作為

國家發展委員會

108 年 3 月

大綱

- GDPR背景
- GDPR重點
- 跨境傳輸議題分析
- GDPR對我國企業之影響
- 政府因應作為
- 結語

GDPR
背景

法規歷程

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
背景

主旨與立法目的

GDPR保護個人基本權與自由，尤其是對於個資自主權的保障

個人資料保護

資料自由流通

GDPR對於個資的保護應無礙於歐盟境內個資的自由流通

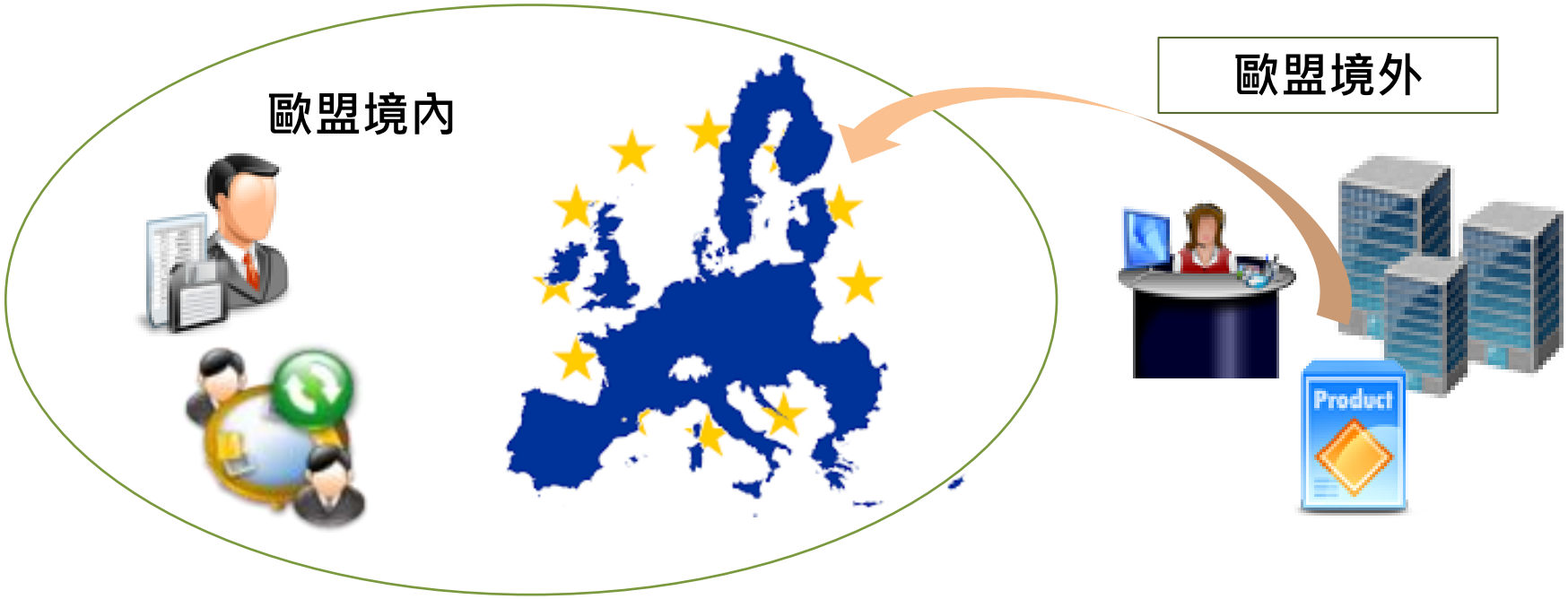
GDPR
重點

適用範圍

主體	地區	行為	資料
• 歐盟境內、外企業皆有適用 • 公、私部門皆有適用	• 以**歐洲經濟區(EEA)**為主，包括歐盟28個會員國、冰島、列支敦斯登與挪威	• 全部或一部以自動化方式處理之個人資料 • 非自動化方式處理而構成檔案系統一部分之個人資料	• 有關識別或可得識別自然人之任何資訊，例如姓名、位置資料、網路識別碼等

GDPR
重點

域外效力



- 設立於歐盟境內之資料控管者（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

域外效力之案例

■本會於2018年7月針對外界詢問國內銀行業適用GDPR之疑義，洽詢歐洲資料保護委員會(EDPB)，EDPB嗣後具體回應我方詢問，並於其2018年底完成之域外效力指引(Guidelines 3/2018 on the territorial scope of the GDPR (Article 3))之草案納入該案例：

…Moreover, it should be noted that the processing of personal data of EU citizens or residents that takes place in a third country does not trigger the application of the GDPR, as long as the processing is not related to a specific offer directed at individuals in the EU or to a monitoring of their behaviour in the Union.

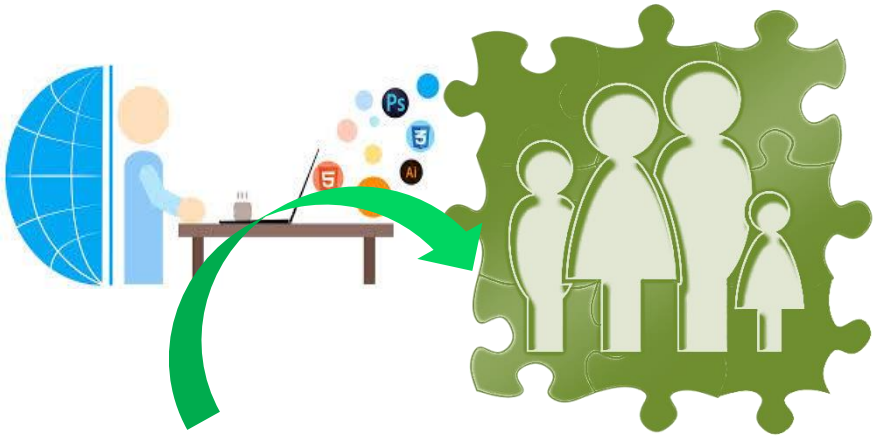
Example 10: A bank in Taiwan has customers that are residing in Taiwan but hold German citizenship. The bank is active only in Taiwan; its activities are not directed at the EU market. The bank's processing of the personal data of its German customers is not subject to the GDPR.

居住台灣的德國公民在台灣的銀行開戶，而該銀行之營運活動未及於歐盟市場，因此該銀行處理個資行為並非直接對歐盟境內特定當事人提供，爰無GDPR之適用。

GDPR
重點

擴大個資定義

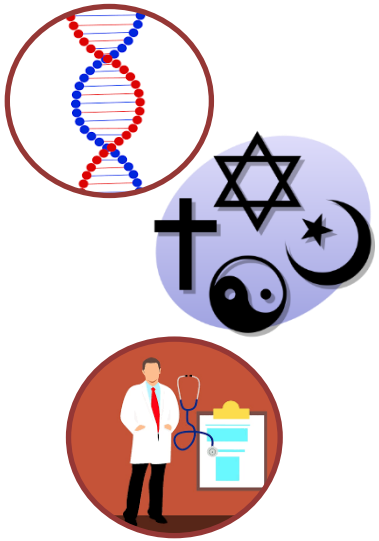
一般個資



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。

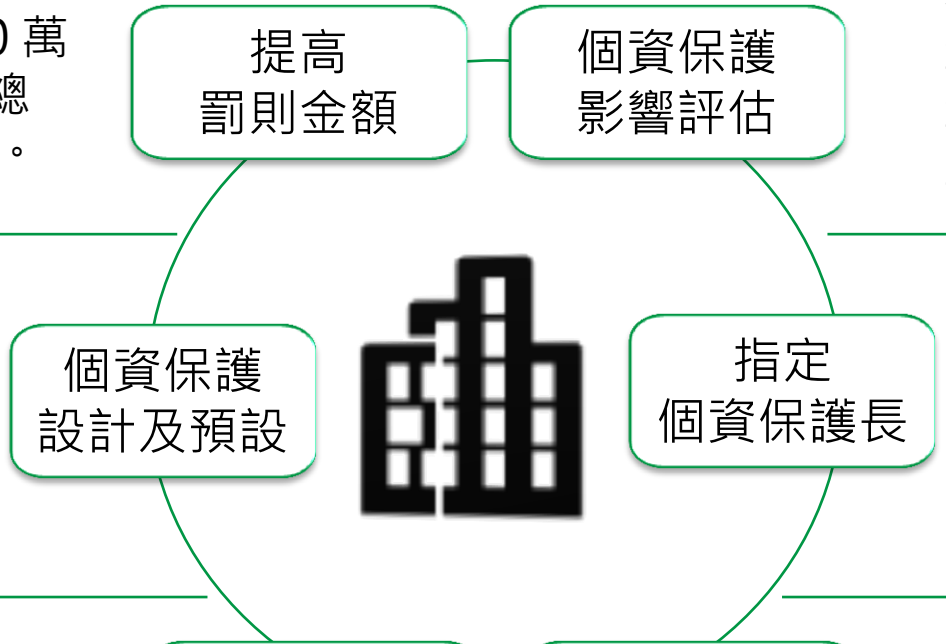
目的：
個人資料之處理具有多重目的者，應就全部目的取得同意。

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。



§25
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

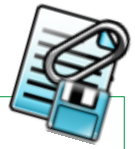
§ 21、22
當事人應有權拒絕對於自動化決策或以任何形式評估個人特徵之建檔行為。

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。

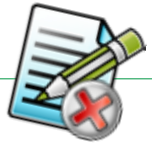
拒絕權

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。

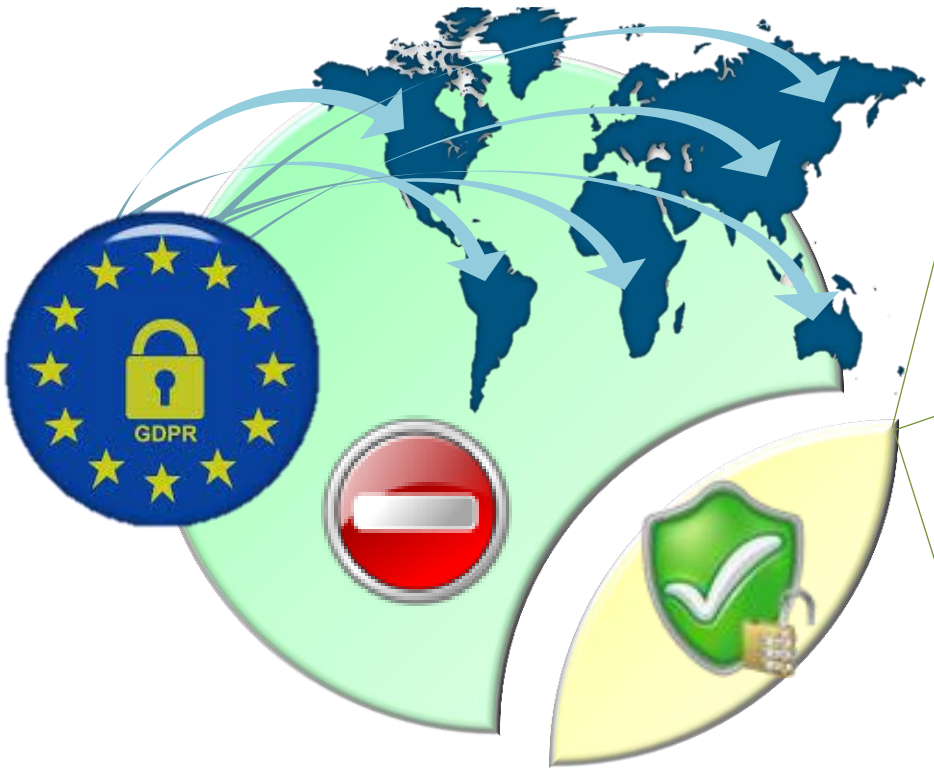
個資
可攜權



§ 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。

跨境傳輸
議題分析

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：
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：

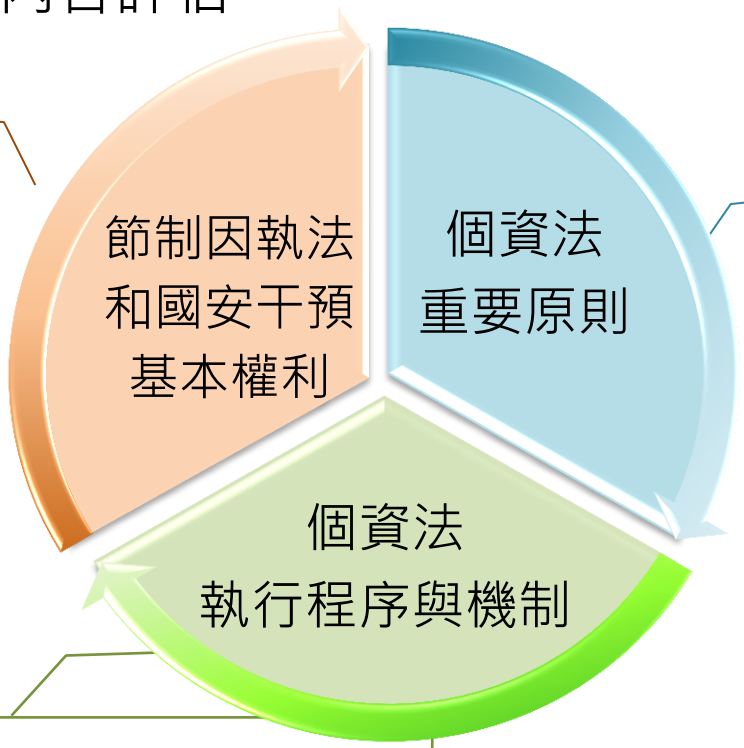
(層次性的規範架構)

- 國家層級：國家取得適足性認定（adequacy decision）
- 企業自我規律：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-評估面向

■ 依 GDPR 條文、第 29 條工作小組 WP 254、WP 237 號文件、歐盟法院 Schrems 案內容評估

- 個資之運用應有法律依據
- 應表明關於合法目的之必要性及合比例性
- 個人資料之運用應受獨立監督
- 應予個資當事人有效之救濟



- 個資保護基本概念
- 合法、公平、合理之方式運用個資
- 目的拘束原則
- 個資品質之確保
- 個資運用須符比例原則
- 限制個資持有期間原則
- 個資安全與保密原則
- 透明原則
- 個資當事人權利
- 跨境傳輸之限制
- 特殊運用原則

- 適當的獨立監督機關
- 個人資料保護機制須確保具有良好的合規性
- 課責機制
- 當事人行使權利及救濟機制

適足性認定-認定程序

申請

- 國家或地區主動提出，雙方展開技術性對話

評估

- 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。

批准

- 歐盟國家代表批准是否具適足性

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）	• 由公協會或代表特定資料處理活動之機構申請 • 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。 • 適合採用之企業：業務僅涉及特定業別。

其他例外情形

- 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。

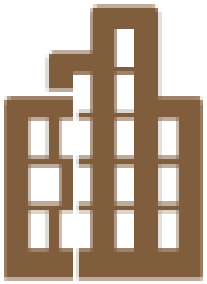
其他例外情形	內容
個資當事人明確同意	告知個資當事人可能之風險後，取得當事人明確同意移轉。
其他必要措施	例如： • 因執行契約所必要。 • 基於公共利益之重要原因。 • 於個資當事人無法為同意之表示，移轉對其有重要利益保護必要。

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）或取得認證（Certification）等 4 種國際傳輸方式，或符合其他例外情形時，始得進行跨境傳輸。

GDPR對我國企業之影響

影響程度



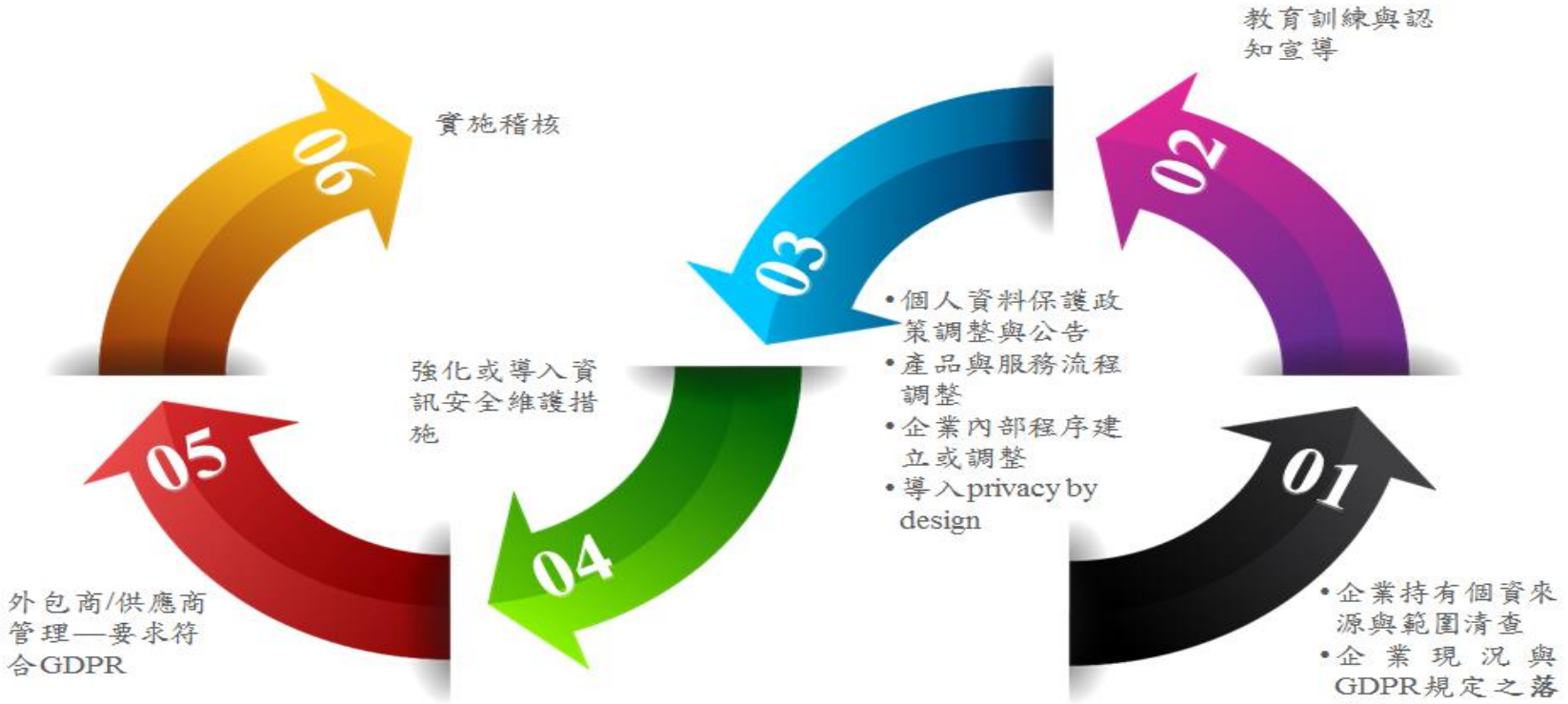
• 非設立於歐盟境內	• 設立於歐盟境內。 • 非歐盟境內，但對歐盟人民提供商品或服務、監控其行為。
• 偶然性處理歐盟個資	• 大規模處理歐盟個資
• 於歐盟境內處理個資	• 進行跨境傳輸
• 使用一般電子處理	• 使用大數據分析或雲端服務
• 在歐盟經濟活動規模較小	• 在歐盟經濟活動規模較大

政府因應作為

產業及相關部會因應措施

■ 經濟部：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
- ✓ 透過**資安服務團**協助產業因應GDPR與促進資安產業發展



【圖示】產業實務做法，資料整理自經濟部「因應GDPR施行之策略與作法」簡報，網址https://www.ndc.gov.tw/Content_List.aspx?n=1DE9FB38844DDC8D

政府因應作為

產業及相關部會因應措施

■ 金管會

一、產業因應情形(以銀行業為例)：於歐盟當地有分支機構者

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。

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。

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）。

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

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。

【圖示】產業實務做法，資料整理自金管會「因應GDPR施行之相關作為」簡報，網址https://www.ndc.gov.tw/Content_List.aspx?n=1DE9FB38844DDC8D

政府因應作為

產業及相關部會因應措施

■ 金管會

二、協助產業因應措施

研討會

- 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。
- 上述二單位共同舉辦「金融業因應歐盟個人資料保護規則」研討會。

交流平台

- 督導銀行公會建置所屬會員公司適用歐盟GDPR規範資訊交流平台。
- 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。

其他

- 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。

政府因應作為

產業及相關部會因應措施

■ 通傳會：盤點產業因應GDPR之需求事項

GDPR議題	業者所需協助作為
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	協助建置管理範本、提供諮詢輔導服務管道及遵法參考指引；行政稽核協助業者完善個資維護機制
跨境傳輸	須確保個資保護已達到「適當之保護水平」，始得傳輸之

產業及相關部會因應措施

■ 交通部

交通部

- 107.05 辦理內部GDPR教育訓練

民航局

- 國籍航空委請顧問公司建置GPDR合規性制度
- 國籍航空辦理教育訓練、修訂隱私權政策並修改網站

航港局

- 台北市海運承攬運送商業同業公會 於 107.07 主辦歐盟個人資料保護規範研討會

觀光旅遊局

- 函請各旅行業、觀光旅遊業及旅館公會向所屬會員宣傳個資保護及GDPR資訊。

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，本會奉行政院指示，於107年7月4日成立「個人資料保護專案辦公室」，工作重點如下：

■整合因應GDPR相關事宜，向歐盟申請適足性認定工作

1.舉辦GDPR研討會及北中南宣導說明會

2.完成適足性評估報告

個資辦公室已啟動向歐方申請適足性認定工作，參考歐盟相關文件，完成適足性評估報告並送交歐方，後續將展開雙方技術性對話。

結語

國發會統籌GDPR事宜

■配合檢討我國個資法，協調整合並加強各部會落實執行個資法之一致性

個資辦公室將因應GDPR適足性認定工作之推動，配合適時檢討我國個資法

就外界提案之個資法疑義，透過邀集相關部會研商討論，以獲共識解決方案

因應數位經濟發展之需求，進行盤點不合時宜之個資法相關函釋

結語

國發會統籌GDPR事宜

■提供GDPR相關重要資訊(1/2)

本會已於官網設置GDPR專區，適時更新 GDPR 相關資訊，包括：

- GDPR 簡介
- GDPR 導讀
- 法規翻譯
- GDPR 與我國個資法之比較分析
- 我國主要部會因應GDPR之作為

網址：https://www.ndc.gov.tw/Content_List.aspx?n=2A22E5DEB45D2552

結語

國發會統籌GDPR事宜

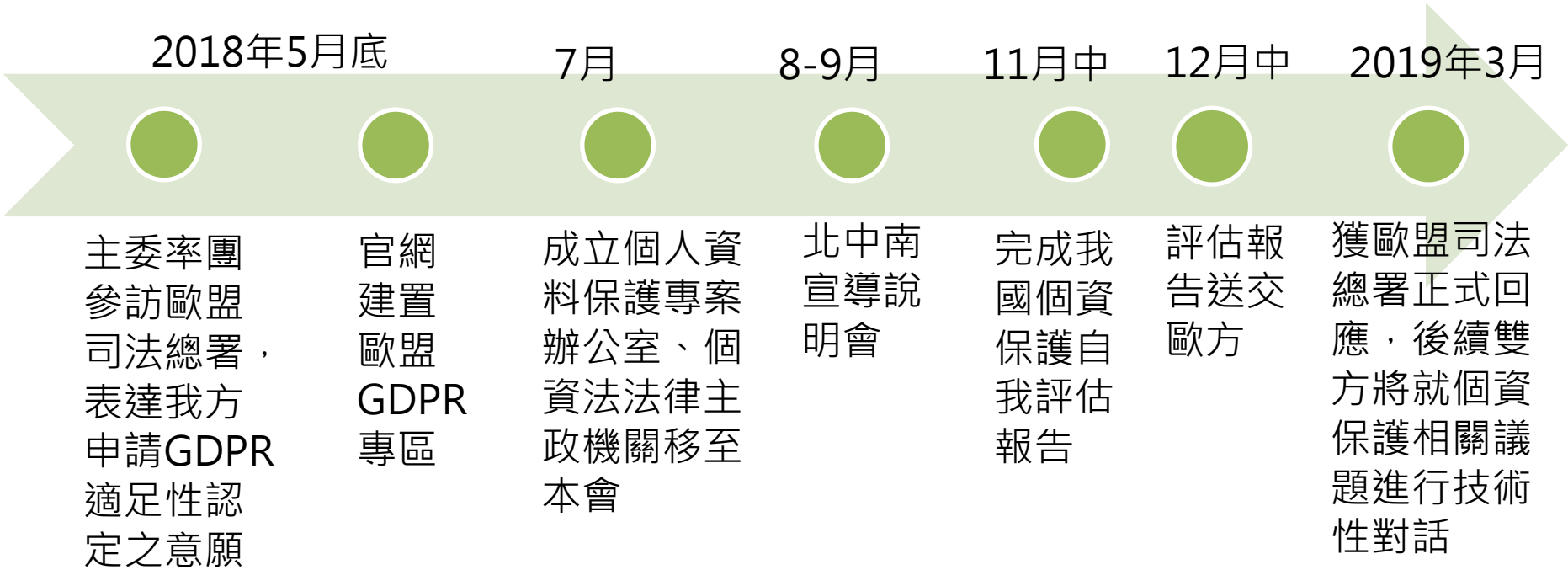
■提供GDPR相關重要資訊(2/2)

本會刻就EDPB已公布/預告之11則指引文件進行翻譯，將於今年陸續完成並置於GDPR專區，俾利外界瞭解GDPR相關條文具體適用情形。

項次	項目	指引
1.	同意	Guidelines on consent under Regulation 2016/679(wp259 rev.01)
2.	GDPR 第 3 條域外效力	Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation
3.	跨境傳輸其他例外情形	Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679
4.	個資侵害事故通報與通知	Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)
5.	個資保護長	Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)
6.	透明原則	Guidelines on transparency under Regulation 2016/679(wp260 rev.01)
7.	個資保護影響評估	Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)
8.	自動化決策及建檔	Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)
9.	個資可攜權	Guidelines on the right to "data portability" (wp242rev.01)
10.	主要監管機關	Guidelines on the Lead Supervisory Authority (wp244rev.01)
11.	行政罰鍰	Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253

結語

國發會統籌GDPR事宜



結語

國發會統籌GDPR事宜

2019年重點工作

與歐方展開技術性對話

持續整合各部會推動GDPR因應事宜

召開專家學者諮詢會議研議個資議題

適時配合檢討我國個資法

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。