Deloitte.

勤業眾信

111年國際個人資料隱私保護（GDPR）推廣說明會

因應GDPR資料跨境傳輸之新議題

勤業眾信聯合會計師事務所 風險諮詢服務/2022.09

講師資料

- 台北市信義區松仁路100號20樓
- Tel：2725- 9988 分機7771
- Fax: 4051- 6888 分機7771
- hanhlin@deloitte.com.tw

林翰

Han Lin

協理

學歷：

臺灣科技大學資管所碩士

臺灣科技大學資管系學士

專業資格：

數據隱私解決方案工程師, CDPSE

ISO 27001 主導稽核員

ISO 27701 主導稽核員

ISO 29100主導稽核員

BS 10012 主導稽核員

ISO 9001 主導稽核員

林翰於2014年進入勤業眾信聯合會計師事務所風險諮詢部門，先前擔任系統分析師一職，主責系統分析與設計，與資訊安全軟體發展導入。在勤業主要提供Cybersecurity安全服務，並主要負責隱私與資料保護相關服務，

內容涵蓋:

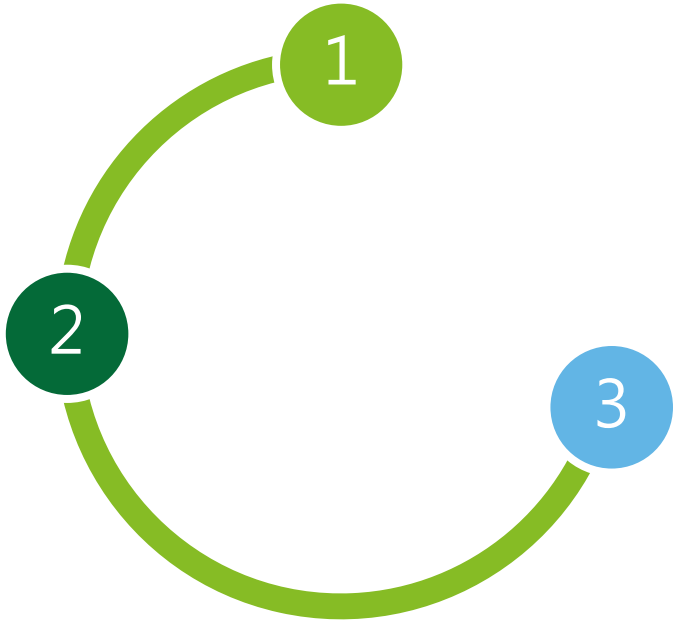
- 隱私保護(含資料去識別化、資料安全治理)、
- 企業營業秘密保護(含: 數據治理及分級控管措施建置)、
- 醫療產業資訊安全保護(含: ISO 27799、上市前資安評估與輔導)、
- Cybersecurity法規適法性諮詢(GDPR、ePrivacy、C-RAF)、
- 企業資訊安全管理與隱私資料保護服務，
- 大資料適法性諮詢、
- 支付信用卡PCI DSS制度建置、IT資訊服務管理制度建置維護(ISO 20000)、安控合規檢測以及其他資訊科技領域的風險管理

經歷：

- 勤業眾信聯合會計師事務所風險諮詢 隱私與資料保護服務 Offering Leader
- 臺灣積體電路製造股份有限公司 系統分析師
- 台灣金融研訓院課程講師

勤業眾信版權所有 保留一切權利

目錄 / CONTENTS



PART 01
隱私保護風險背景

- 本節主要介紹全球隱私保護全景與背景。

PART 02
主要跨境資料傳輸趨勢

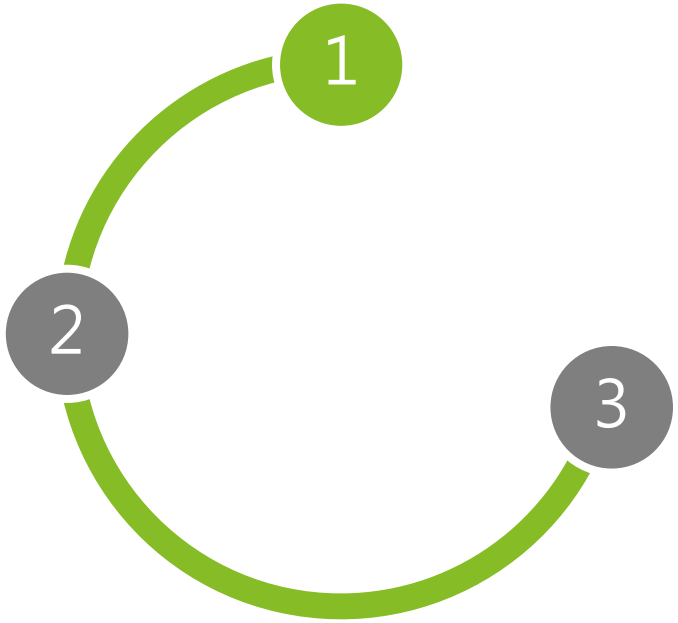
- 本節主要介紹各國主要針對跨境資料傳輸議題之要求與執行重點

PART 03
跨境資料傳輸趨勢實施方案

- 本節主要介紹因應跨國企業針對資料跨境傳輸前後隱私與資訊安全相關要求，業者該如何落實。

勤業眾信版權所有 保留一切權利

目錄 / CONTENTS



PART 01
隱私保護風險背景

- 本節主要介紹全球隱私保護全景與背景。

PART 02
主要跨境資料傳輸趨勢

- 本節主要介紹各國主要針對跨境資料傳輸議題之要求與執行重點

PART 03
跨境資料傳輸趨勢實施方案

- 本節主要介紹因應跨國企業針對資料跨境傳輸前後隱私與資訊安全相關要求，業者該如何落實。

勤業眾信版權所有 保留一切權利

身處數位時代的今日，各類網路安全威脅蠢蠢欲動

在現今數位時代，Cyber Everywhere。網路安全風險已與日常生活各種構面共存。

Cyber Risk不僅僅是資訊科技
(Information Technology)

Cyber Risk不僅框在
資料中心 / 資訊單位

Cyber Risk不僅包含
內部員工

Cyber is **complex.**

Cyber is **ever-changing.**

Cyber is **everywhere.**

Cyber **everywhere.**

Innovate **anywhere.**

網路安全對於企業的挑戰 – 網路風險管理能力追不上數位創新發展需求

網路風險管理正在不斷發展，下一階段，企業面臨的將是管理無法控制的風險

Cyber Everywhere. Risk Everywhere.

隱私不僅是合規問題，需要透過多角度檢視

We help our clients think about privacy as more than just compliance.

勤業眾信版權所有 保留一切權利

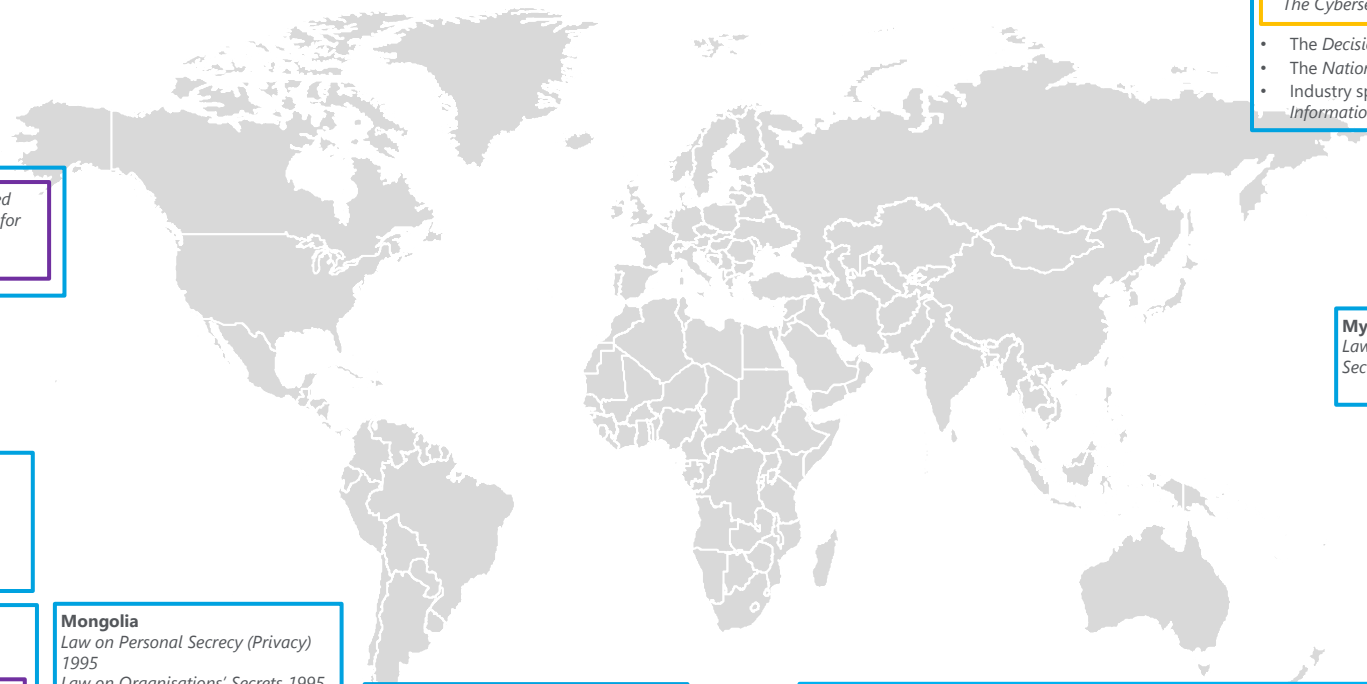
立足台灣，放眼全球，隱私保護議題是全球議題

在數位時代中，
企業通常具有**跨境維度**

企業的跨境規模
會給企業隱私資料帶來**風險**

了解整體全貌隱私保護風險
將為企業全球隱私策略提供參考

Key
- 既有法規
- 近年新法規
- 草案討論



United States of America
California Consumer Privacy Act 2018 (California)
- *Data Care Act 2018*

Brazil
General Data Protection Law 2018

South Africa
The Protection of Personal Information Act 2013

Singapore
Personal Data Protection Act 2012
- *Cybersecurity Act 2018*
- *Regulator released discussion paper for uplift – data portability?*

Taiwan
Personal Information Protection Act 2010

Macau
Personal Data Protection Law 2005

India
No specific privacy law - a set of Rules made under *the Information Technology Act 2000* resemble a data privacy law.
- *Personal Data Protection Bill 2018*

Japan
Act on the Protection of Personal Information 2003 – Received significant uplift in 2017
- *Agreed supplementary rules to obtain adequacy decision*

Mongolia
Law on Personal Secrecy (Privacy) 1995
Law on Organisations' Secrets 1995

Laos
The Law on Electronic Data Protection 2017

Malaysia
Personal Data Protection Act 2010
- *Under review by Ministry of Communications and Multimedia*

Hong Kong
Personal Data (Privacy) Ordinance 1996

Philippines
Data Privacy Act of 2012

Europe
General Data Protection Law 2018
Member State Laws i.e Data Protection Act 2018 (UK)

China
Significant uplift in recent years including:
- *The Cybersecurity Law (2016)*
- The *Decision on Strengthening Online Information Protection (2012)*
- The *National Standard of Security Technology (2012)*
- Industry specific requirements (i.e. *Rules Regarding the Protection of Personal Information of Telecommunications and Internet Users 2013)*

South Korea
Personal Information Protection Act 2011
- *Act on the Promotion of IT Network Use and Information Protection (Network Act) in December 2018*

Myanmar
Law Protecting the Privacy and Security of Citizens, 2017

Thailand
Personal Data Protection Act, 2019
Cybersecurity Act, 2019

Vietnam
Law on Network Information Security, 2015
- *Law on Cybersecurity 2018*

Indonesia
No specific privacy law - the *Electronic Information and Transaction Law* (EIT Law) contains provisions relating to electronic data only
- *Draft Data Protection Law– early 2019*

Australia
Privacy Act 1988 (Cth) incl. State privacy laws, surveillance laws
- *Notifiable Data Breaches Scheme Federal Public Sector Code 2017*
- *Consumer Data Right Bill 2019*
- *GDPR-like law? Privacy Code?*

New Zealand
Privacy Act 1993 (Cth)
- *Privacy Bill under review*

勤業眾信版權所有 保留一切權利

資料須得以自由運用與流動，才能最大化資料的價值

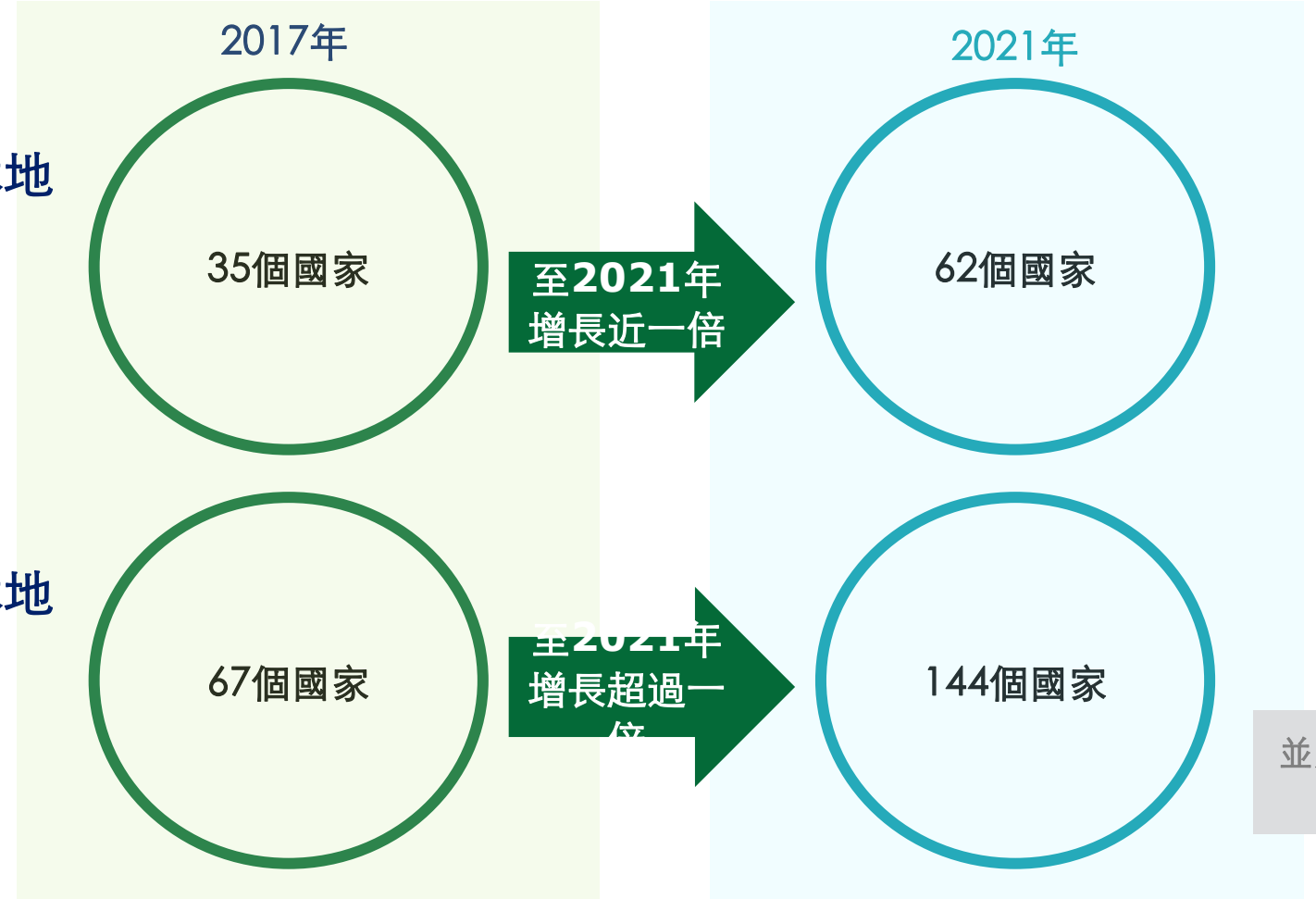
資料流動有助於創新與經濟成長

勤業眾信版權所有 保留一切權利

然而因資料分享在創造價值的同時亦產生隱私風險，導致各國逐漸傾向資料本地化(Data Localization)

2017年全球實施資料本地化規範的國家

2017年全球制訂資料本地化規範的國家總數



並另有38部政策已被提案或考慮中。

中國、印度、俄羅斯、土耳其分別居於全球強制資料本地化的國家前幾位。

勤業眾信版權所有 保留一切權利

促進資料流動、增進資料跨境分享，將可透過資料利用使資料價值最大化，同時對市場帶來利益

Cisco Consumer Privacy Survey

84% 的受訪者表示，他們關心個人資料與隱私，並且希望更好地管控資料的使用方式

48% 對個人隱私保護持積極態度的受訪人中，有**48%**曾因為公司資訊政策或資料共享政策更換服務提供商

61% **61%**的受訪者表示，對個人隱私保護持積極態度的受訪人年齡在**45**歲以下

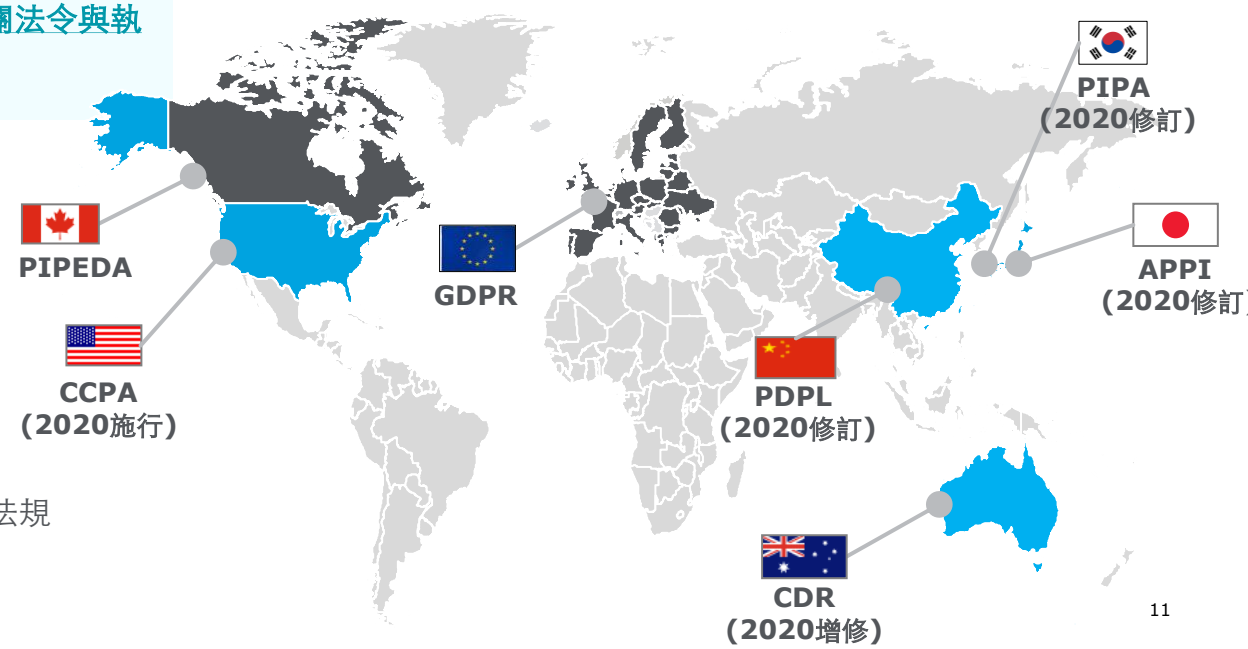
資料來源: Cisco Cybersecurity Series 2019、國發會個人資料保護專區

個人資料保護法

NT$ 20m 若違反個資法，針對同一事件最高可依民事責任罰2億新台幣

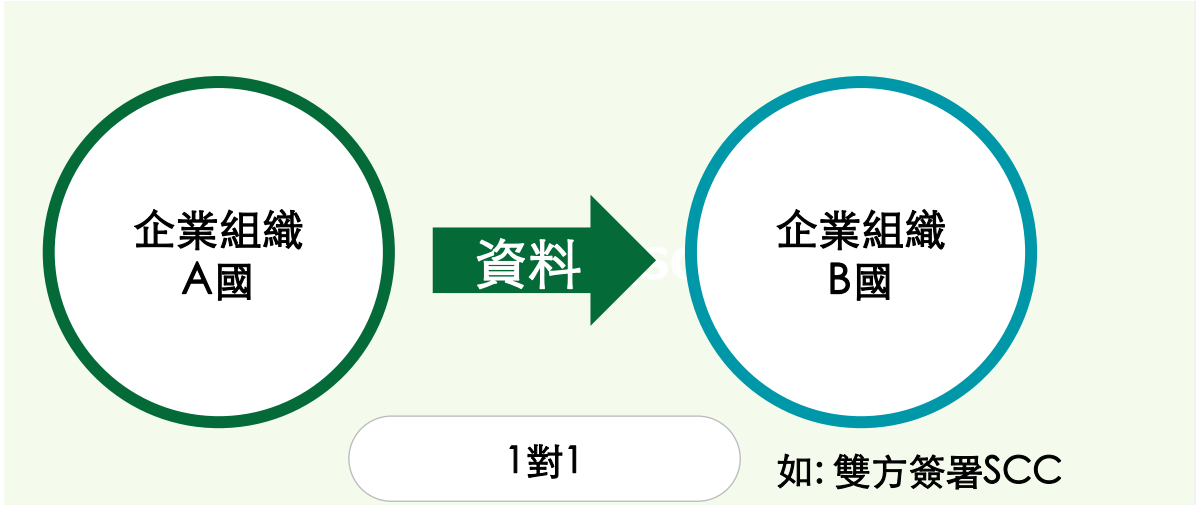
10 自個資法於民國101年施行以後，每年約新發布10項個資相關法令與執行措施

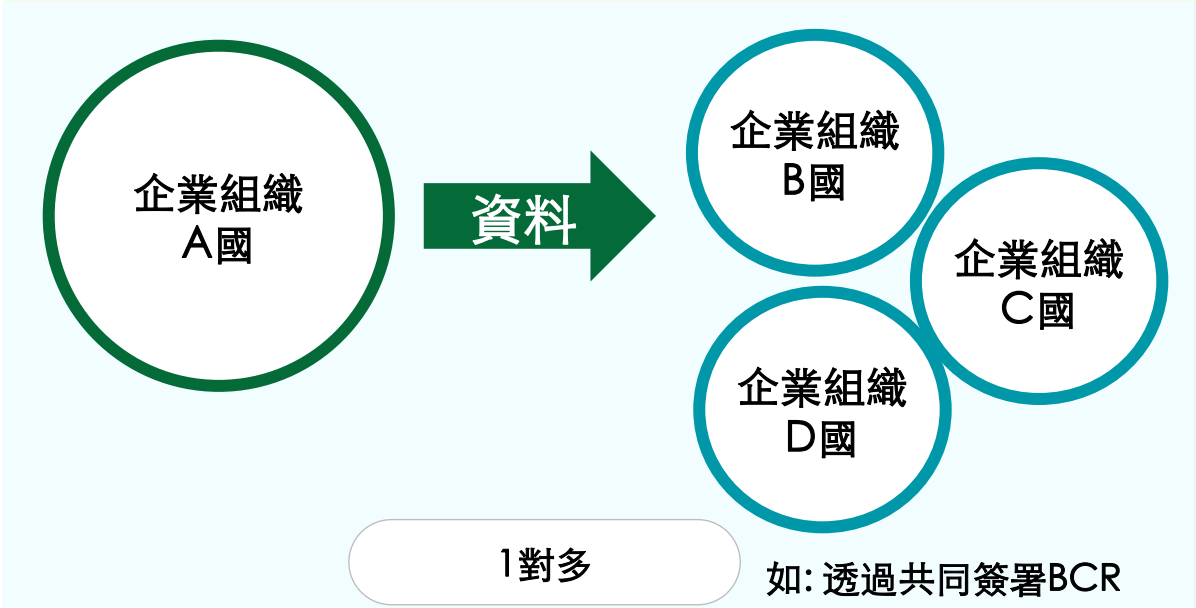
各國個資相關法規



勤業眾信版權所有 保留一切權利

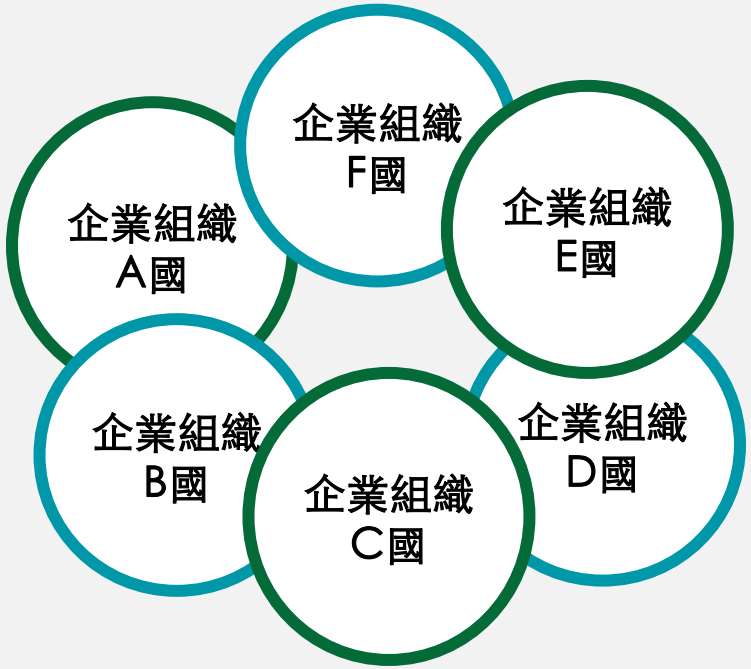
資料跨境分享情境





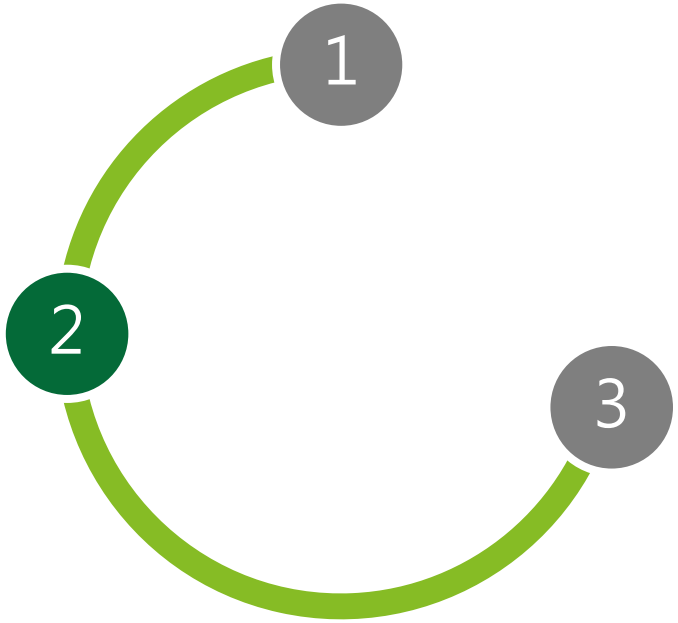
多對多

如：各國家加入相同協議或組織，取得認證，如CBPR



勤業眾信版權所有 保留一切權利

目錄 / CONTENTS



PART 01
隱私保護風險背景

- 本節主要介紹全球隱私保護全景與背景。

PART 02
主要跨境資料傳輸趨勢

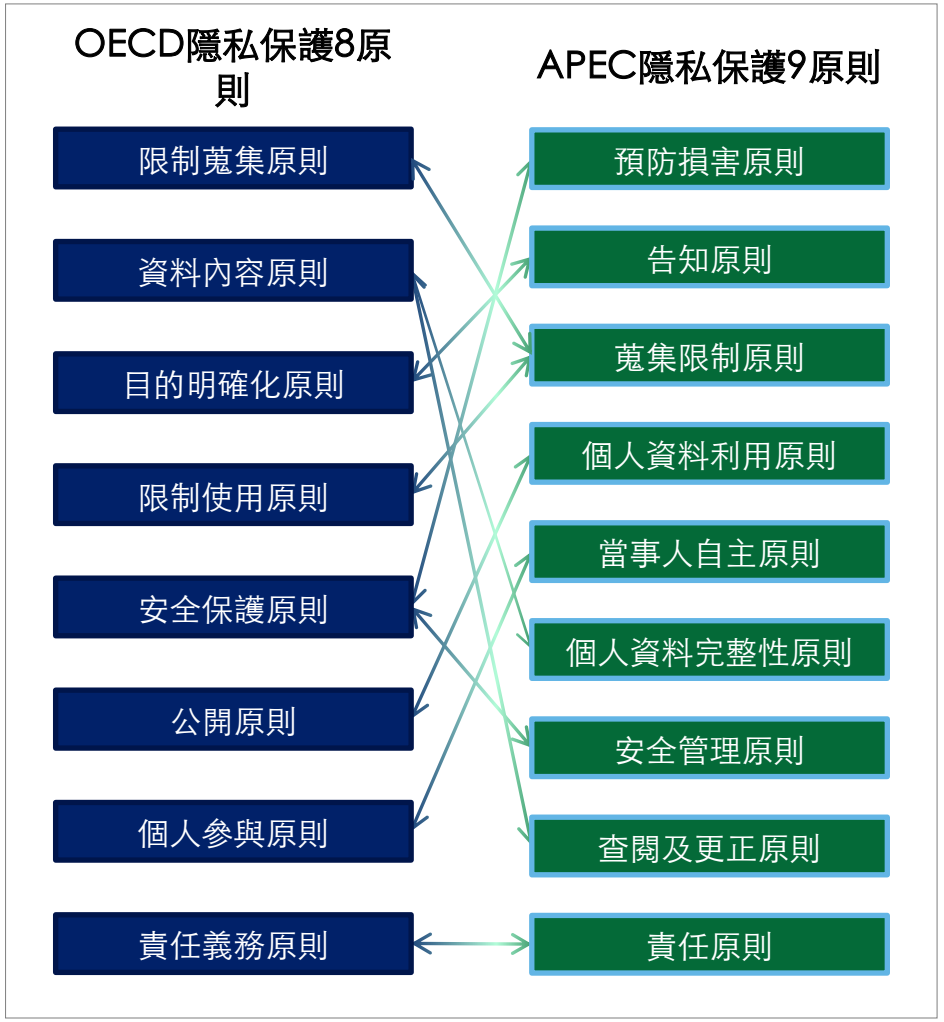
- 本節主要介紹各國主要針對跨境資料傳輸議題之要求與執行重點

PART 03
跨境資料傳輸趨勢實施方案

- 本節主要介紹因應跨國企業針對資料跨境傳輸前後隱私與資訊安全相關要求，業者該如何落實。

勤業眾信版權所有 保留一切權利

各國隱私法規源頭 - OECD 隱私保護原則



OECD 隱私保護8原則	說明
限制蒐集原則	個人數據的收集應受到限制，任何此類數據均應通過合法，公正的手段，並在適當情況下，在數據主體知情或同意的情況下獲得。
資料內容原則	個人數據應與使用目的有關，並且在達到這些目的所必需的範圍內，應準確，完整併保持最新。
目的明確化原則	收集個人數據的目的應不遲於收集數據時指定，隨後的使用應僅限於實現這些目的或與這些目的不兼容並在每種情況下規定的其他目的目的改變。
限制使用原則	除根據告知之的目的外，不得披露，提供或以其他方式使用個人數據，但以下情況除外: a）在數據主體的同意下；或 b）由法律授權。
安全保護原則	個人數據應受到合理的安全保護措施的保護，以防止丟失或未經授權的訪問，破壞，使用，修改或披露數據的風險。
公開原則	對於個人數據的發展，做法和政策，應該有一個開放的一般政策。應該易於獲得確定個人數據的存在和性質，使用它們的主要目的以及數據控制者的身份和慣常住所的手段。
個人參與原則	應提供數據提供個人對於其提供之數據之參與權
責任義務原則	數據控制者應負責遵守實現上述原則的措施

勤業眾信版權所有 保留一切權利

各重點國家隱私保護法規比較 (國際跨境傳輸)

	台灣	中國	歐盟	美國	日本	新加坡	印度
名稱	個人資料保護法	網路安全法	一般資料保護規範GDPR	《健康保險隱私及責任法案》HIPPA	個人資料保護法	個人資料保護法 PDPA	Personal Data Protection Bill
範圍	公務機關/ 私人企業/ 屬地	公務機關/ 私人企業/ 屬地	公務機關/ 私人企業/ 屬地	直接處理病患資料的醫院、醫療服務提供者、雇主贊助醫療計劃、研究機構和保險公司	公務機關/ 私人企業/ 屬地	私人企業/ 屬地	公務機關/ 私人企業/ 屬地
目的著重	促進個資之合理利用	保護個資當事人之權利	保護個資當事人之權利	保障勞工權利	保障個人權益	強化經濟競爭力與地位	保護個資當事人之權利
特別的個資定義	略	未定義	種族、信仰、工會、Cookie、IP及GPS…等	醫療資訊	人種、信仰、社會身分	未定義 敏感性個資	財務資訊、密碼、健康資料、基因、性傾向、生物資訊、兒童資訊
國際傳輸	原則開放、例外禁止(第21條)	原則禁止、例外開放(第37條)	原則禁止、例外開放(BCR/SCC…)	合規後可用上雲服務	原則禁止、例外開放(第24條)	達到基本要求即可傳輸	原則禁止、例外開放(SCC…)
主管機關	依行業別而定	中央網絡安全和信息化委員會辦公室	各國指定之DPA	略	個人情報保護委員會	個人資料保護委員會(PDPC)	Data Protection Authority
通報主管機關	行政院及所屬各機關落實個人資料保護聯繫作業要點	安全事件通報、個人資訊和重要數據出境安全評估	個資外洩、DPIA高風險事項徵詢	必須向其涵蓋的實體或業務關聯客戶報告安全事件	無特別要求	無特別要求	個資外洩、跨境傳輸
特色措施	略	網路實名制、網路數據安全、數據落地	DPO、PbD、資料可攜、拒絕自動化決策及剖析	CSP雲指南	JISQ 15001 隱私標誌制度	謝絕來電計劃、保護年限100年	DPO、PbD、Data storage imitation

隱私資料跨境傳輸要求— 歐盟

勤業眾信版權所有 保留一切權利

隱私資料跨境傳輸要求— 日本

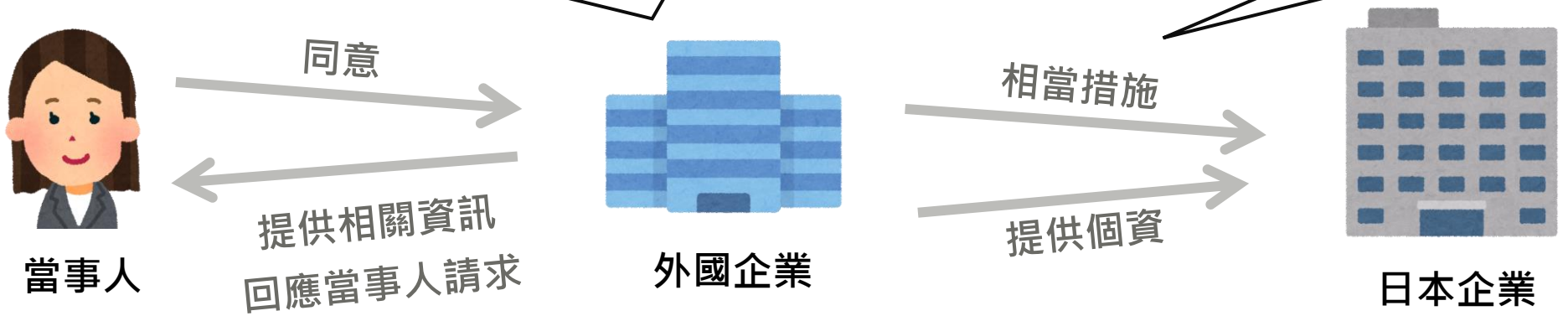
1 取得當事人同意

- 取得同意時，須提供當事人資料接收方所在之國家、資料接收方關於個資保護之制度、資料接收方對於個資保護所實施之控制措施等資訊並使其知悉

2 實施相當控制措施

- 與資料控制者一同採取適當且合理的措施（如資料傳輸方取得CBPR認證，而資料接收方係為資料處理者，亦是適當也合理措施之一）
- 資料接收方取得個資保護相關之國際認定（如CBPR之認證）

- 如出現障礙，應採取必要且適當之對應。
- 如難以確保可持續執行該措施，應暫停提供資訊。



*當在外國處理個人資料之企業向日本人（如日本居民）提供商品或服務係與日本人個人資訊相關時，將受《個人資料保護法》域外效力之限制。

勤業眾信版權所有 保留一切權利

隱私資料跨境傳輸要求— 日本

1 取得當事人同意

- 取得同意時，須提供當事人資料接收方所在之國家、資料接收方關於個資保護之制度、資料接收方對於個資保護所實施之控制措施等資訊並使其知悉

2 實施相當控制措施

- 與資料控制者一同採取適當和合理的措施（如資料傳輸方取得CBPR認證，而資料接收方係為資料處理者，亦是適當和合理措施之一）
- 資料接收方取得個資保護相關之國際認定（如CBPR之認證）
- 如出現障礙，應採取必要和適當的對應。
- 如難以確保持續執行該措施，應暫停提供資訊

3 與日本有相當程度之個資保護制度

- 冰島、愛爾蘭、義大利、英國、愛沙尼亞、奧地利、荷蘭、賽普勒斯希臘、克羅埃西亞、瑞典、西班牙、斯洛伐克、斯洛維尼亞、捷克、丹麥、德國、挪威、匈牙利、芬蘭、法國、保加利亞、比利時 、波蘭、葡萄牙、馬爾他、拉脫維亞、立陶宛、列支敦士登、羅馬尼亞、盧森堡→維持原施行方法

*當在外國處理個人資料之企業向日本人（如日本居民）提供商品或服務係與日本人個人資訊相關時，將受《個人資料保護法》域外效力之限制。

勤業眾信版權所有 保留一切權利

隱私資料跨境傳輸要求— 中國

個人信息原則應存放在中華人民共和國境內，個人信息處理者因業務等需要，確需向中華人民共和國境外提供個人信息的，應當具備下列條件之一：

依照第四十條的規定通過國家網信部門組織的安全評估

按照國家網信部門的規定經專業機構進行個人信息保護認證

關鍵信息基礎設施運營者和處理個人信息達到國家網信部門規定數量的個人信息處理者，應當將在中華人民共和國境內收集和產生的個人信息存儲在**境內**

按照國家網信部門制定的標準合同與境外接收方訂立合同，約定雙方的權利和義務。

法律、行政法規或者國家網信部門規定的其他條件

勤業眾信版權所有 保留一切權利

隱私資料跨境傳輸要求— 中國

數據出境安全評估報告要求及內容

向境外提供個人信息和重要數據的數據處理者

數據安全評估

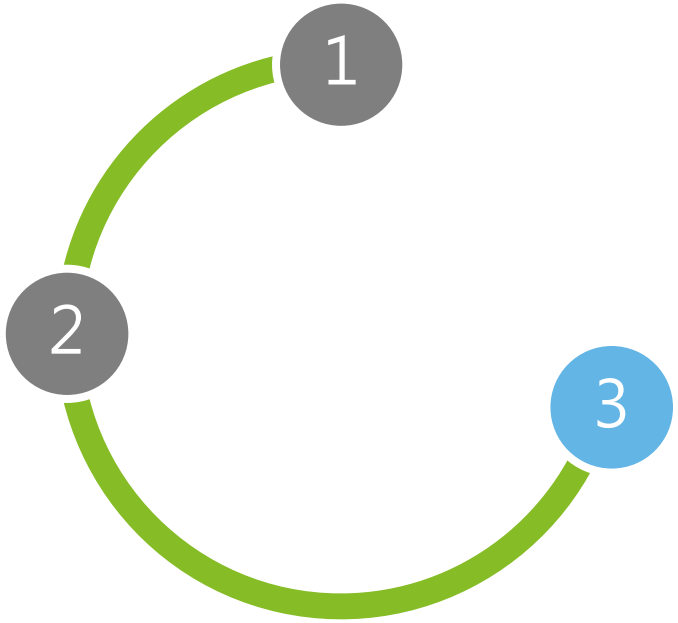
市級網信部門

年度數據出境情況：

- 全部數據接收方的名稱、聯繫方式
- 出境數據的類型、數量和目的
- 數據在境外的存放地點、存儲期限、使用範圍和方式
- 涉及向境外提供數據的用戶投訴及處理狀況
- 發生的數據安全事件及處理狀況
- 數據出境後再轉移之狀況
- 國家網信部門明確向境外提供數據需要報告的其他事項。

勤業眾信版權所有 保留一切權利

目錄 / CONTENTS



PART 01
隱私保護風險背景

- 本節主要介紹全球隱私保護全景與背景。

PART 02
主要跨境資料傳輸趨勢

- 本節主要介紹各國主要針對跨境資料傳輸議題之要求與執行重點

PART 03
跨境資料傳輸趨勢實施方案

- 本節主要介紹因應跨國企業針對資料跨境傳輸前後隱私與資訊安全相關要求，業者該如何落實。

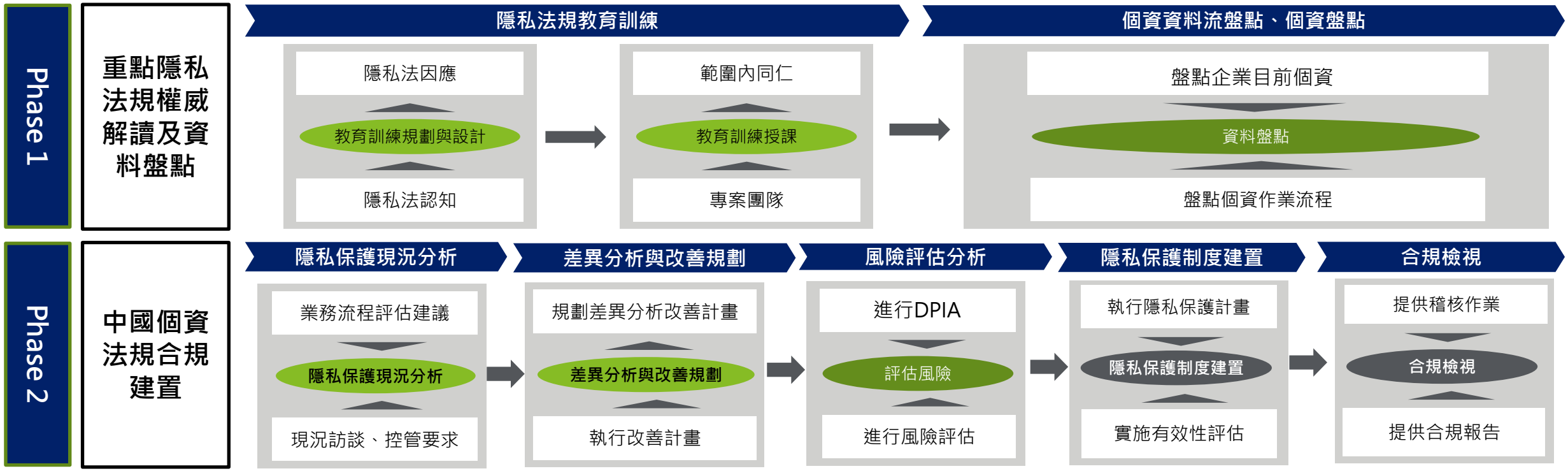
勤業眾信版權所有 保留一切權利

跨境資料傳輸趨勢實施方案 - (已建立PIMS制度組織者)

◆專案階段◆	◆主要工作項目◆	◆預期效益◆
Phase 01 **重點隱私法規權威解讀及資料盤點**	使客戶了解須符合跨境之隱私法知識，並開始進行個人資料盤點，以強化組織內部管理控制	藉由比較、了解所需符合跨境之隱私法來了解相關的框架、內容、精神以及內部需求，接著的資料盤點為下段奠下基礎及準備。
Phase 02 **法規合規建置**	• 執行資料流以及盤點分析 • 執行跨境隱私法差異分析及提供改善計畫 • 執行DPIA與風險評估 • 建立隱私保護政策 • 建置公司層級保護框架 • 執行有效性評估以及合規檢視	以遵法為前提，透過隱私保護管理組織的建立，平衡控管與業務發展的雙重考量，建立管理制度框架，以同時符合我國個資管理與他國個資法要求。

勤業眾信版權所有 保留一切權利

專案實施規劃概覽 - (已建立PIMS制度組織者)



勤業眾信版權所有 保留一切權利

專案實施規劃概覽 - (尚未建立PIMS制度組織者)

第一階段	第二階段	第三階段	第四階段	第五階段
專案規劃階段	管理制度現況 了解與制度強化	內部查核	外部查核	專案結案
提出專案執行計畫書	辨識個人資料 相關業務流程	查核底稿製作	介接認證服務	個人資料保護技術 移轉
專案啟動會議	執行個人資料 保護現況訪談	擬定內部查核計畫	認證準備與顧問諮詢	結案會議
	執行個資管理制度 差異分析	執行內部查核計畫	實地認證與顧問陪同	
	提供個人資料保護角色 、組織與權責建議	發現事項與改善建議	審查結果發現事項 建議與矯正預防	
		管理審查會議		

專案溝通、管理及技術轉移

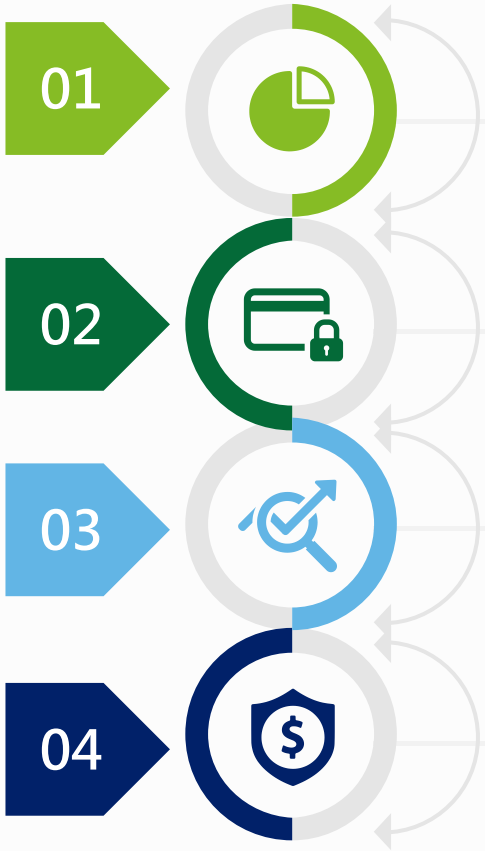
隱私資訊管理教育訓練規劃與執行

勤業眾信版權所有 保留一切權利

跨境傳輸關鍵三步驟— 1. 業務流程盤點

隱私業務場景盤點：執行隱私資料盤點時，先通過業務流程圖識別出包含隱私資料處理的業務場景，及場景中處理隱私資料的部門和系統，如某公司業務流程，其業務場景盤點步驟如下：

業務場景拆分步驟



Level 1: 框定某公司整體業務範圍，可分為註冊、行銷、流覽、下標、支付、物流、客服、資料主體權利9大業務模組。

Level 2：在Level 1的基礎上拆分出物流業務場景

Level 3：在level 2的基礎上識別物流業務場景中具體執行階段和執行活動

根據確定和劃分的level 1，level 2，level 3繪製業務流程圖

流程拆分歸納

劃分業務模組（Level 1）

確定業務場景（Level 2）

劃分業務流程階段(Level 3)

→ 業務流程圖

流程拆分資訊匯總示例

I.業務流程資訊

Code	Level1	Code	Level2	Code	Level3	Code	Level4
01	保單行政作業	04	保全管理	05	保單借款對帳		保單借款(支票件)
01	保單行政作業	04	保全管理	06	媒體扣款作業		媒體扣款作業
01	保單行政作業	04	保全管理	07	保單借款對帳		虛擬還款帳務作業
01	保單行政作業	04	保全管理	08	電腦派員送金單作業		N/A
01	保單行政作業	04	保全管理	09	保單借款還款作業		N/A
01	保單行政作業	04	保單貸款	10	保單貸款利息資本化作業		N/A
01	保單行政作業	04	保全管理	11	保單借款對帳		借款餘額不平作業
01	保單行政作業	04	保單貸款	12	借款總額明細對帳作業		N/A
01	保單行政作業	04	保單貸款	13	借據歸檔、催辦作業		N/A
01	保單行政作業	04	保全管理	14	保單借款對帳		虛擬還款收據列印作
01	保單行政作業	04	保單貸款	15	壽險保單催告、停效		催告與停效作業

示例

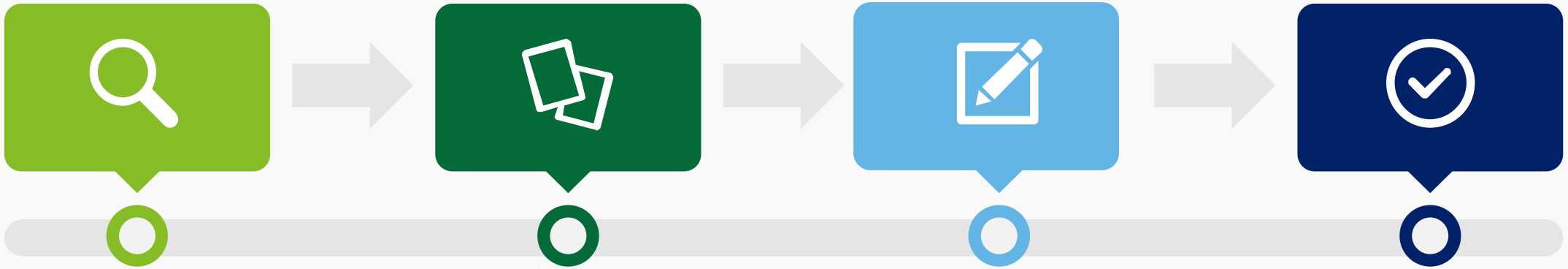
Next:以業務流程階段（即Level 2）為單位進行**業務流圖、資料流程圖BIF的**繪製

勤業眾信版權所有 保留一切權利

跨境傳輸關鍵三步驟— 2. 資料盤點

隱私資料盤點：識別出涉及隱私資料的業務場景後，通過資料流程圖（BIF圖）整理隱私資料的收集、儲存、使用、傳輸隱私資料等處理活動及處理活動涉及的部門或系統，如某公司業務流程的BIF圖，其繪製方法如下：

BIF圖繪製步驟



Step 1

識別某公司業務流程中隱私資料處理活動所涉及的部門、系統及相關協力廠商。

Step 2

整理物流流程中涉及的隱私資料及其在生命週期內的完整流向。

Step 3

按照識別和整理出的部門、系統、相關協力廠商、隱私資料流程向繪製BIF圖。

Step 4

檢查隱私資料流程向是否繪製完整，以確保物流流程中所有涉及的隱私資料、系統、部門及協力廠商均被識別。

勤業眾信版權所有 保留一切權利

跨境傳輸關鍵三步驟— 3. 跨境方案選定實施流程

某公司各業務方應遵守中跨境傳輸相關要求，確保存在適當的跨境傳輸合法依據後，方可將隱私執行跨境傳輸。

跨境傳輸應對流程

Step 1　整理資料跨境的業務場景

隱私保護執行小組

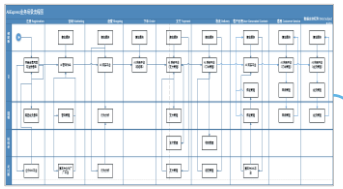
Step 2　評估和選擇適用的跨境傳輸合法依據

隱私保護推行小組法務

Step 3　執行或規劃適用的應對方案

隱私保護執行小組

1-1 整理並標記涉及跨境的**業務場景**



1-2 識別跨境場景中涉及的**資料接收方和資料類型**

1 根據跨境場景描述，**整理匯整涉及的法規要求。**

PIPL　GDPR

結合法規要求和某公司的隱私保護現況，**分析使用的合法依據。**

法規依據 ＋ 隱私現況

適用依據

方案A

每次跨境傳輸資料時，與資料接收方簽署法務團隊提供的**標準合約條款（SCC/GDPR/PIPL/CN）**，來滿足跨境傳輸資料保護要求。

方案B...N

考慮相關跨境傳輸標準，如(CBPR)以確保需跨境保護之國家法規要求之合規(日本/新加坡)

勤業眾信版權所有 保留一切權利


Q&A

Deloitte.

勤業眾信

Deloitte泛指Deloitte Touche Tohmatsu Limited（簡稱"DTTL"），以及其一家或多家全球會員所網絡及其相關實體（統稱為"Deloitte組織"）。 DTTL（也稱為"Deloitte 全球"）每一個會員所及其相關實體均為具有獨立法律地位之個別法律實體，彼此之間不對第三方承擔義務或約束。 DTTL每一個會員所及其相關實體僅對其自身的作為和疏失負責，而不對其他的作為承擔責任。 DTTL並不向客戶提供服務。 更多相關資訊，請參閱www.deloitte.com/about 了解更多。

Deloitte 亞太(Deloitte AP)是一家私人擔保有限公司，也是DTTL的一家會員所。Deloitte 亞太及其相關實體的成員，皆為具有獨立法律地位之個別法律實體，提供來自100多個城市的服務，包括：奧克蘭、曼谷、北京、河內、香港、雅加達、吉隆坡、馬尼拉、墨爾本、大阪、首爾、上海、新加坡、雪梨、台北和東京。

本出版物係依一般性資訊編寫而成，僅供讀者參考之用。Deloitte Touche Tohmatsu Limited（簡稱"DTTL"）、其會員所或其相關實體的全球網路（統稱為"Deloitte組織"）均不透過本出版物提供專業建議或服務。 在做出任何決定或採取任何可能影響企業財務或企業本身的行動之前，請先諮詢合格的專業顧問。

對於本出版物中資料之準確性或完整性，不作任何陳述、保證或承諾（明示或暗示），DTTL、其會員所、相關實體、僱員或代理人均不對與依賴本出版物的任何人直接或間接引起的任何損失或損害負責。 DTTL及其每個成員公司及其相關實體在法律上是獨立的實體。

© 2022 勤業眾信版權所有 保留一切權利

Deloitte.

勤業眾信

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2022 Deloitte Asia Pacific Services Limited.