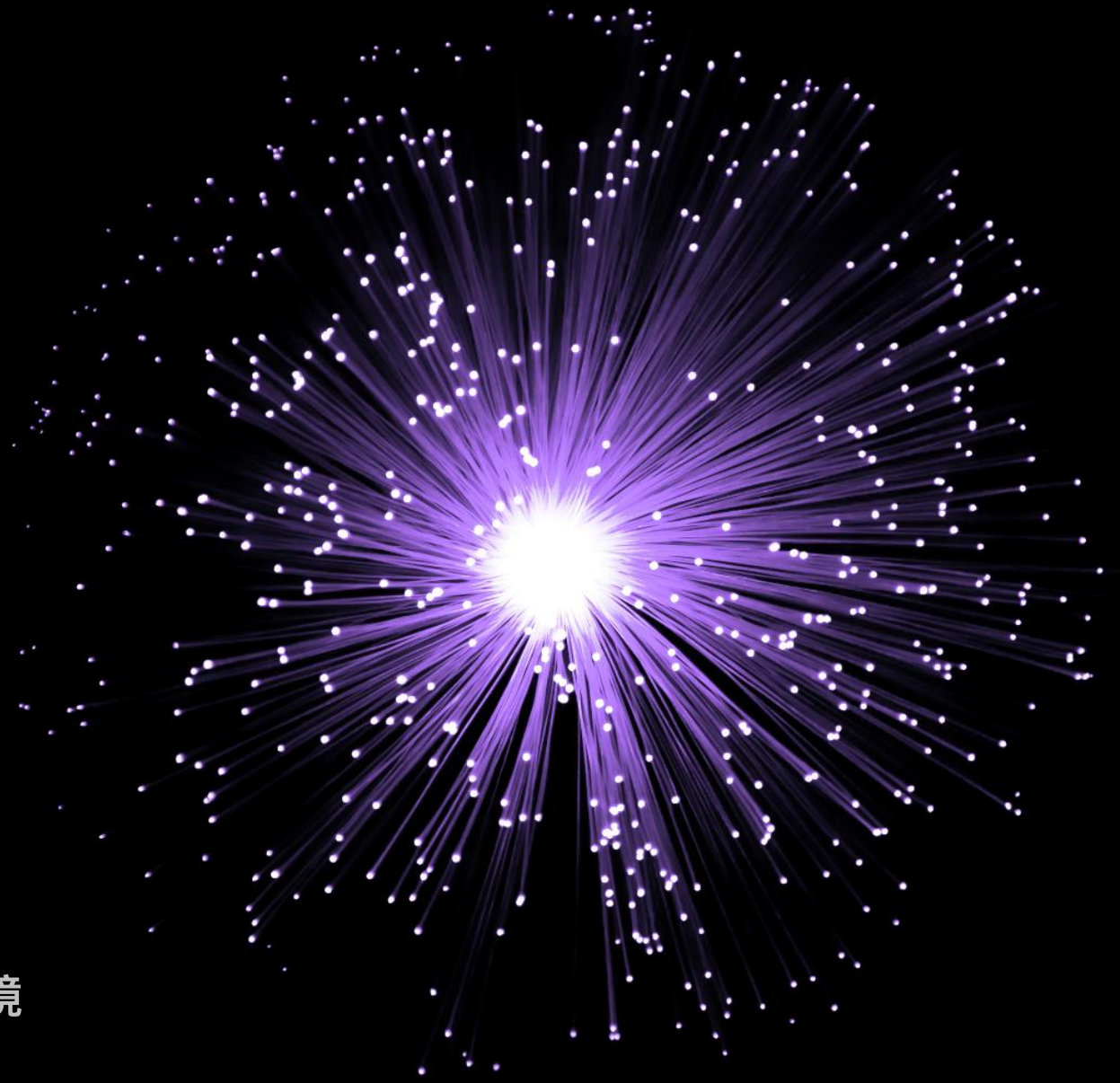
Deloitte.

勤業眾信



個人資料稽核實務與困境

報告人：萬幼筠

2019.11.26

報告人員簡歷

萬幼筠

現職
- 東吳大學法律研究所科技法律組 - 兼任助理教授
- Deloitte Risk Advisory – 執行副總經理

參與專業組織
- 國際資訊系統稽核協會(ISACA)
- 國際舞弊偵防協會(ACFE)
- 國際資訊安全專家協會(ISC2)
- 中華民國資訊服務管理協會(ITSMA)
- 台灣舞弊防治與鑑識協會 (ACFD)
- 中華民國科技法律經理人協會(TILO)
- 美國計算機協會 (ACM)

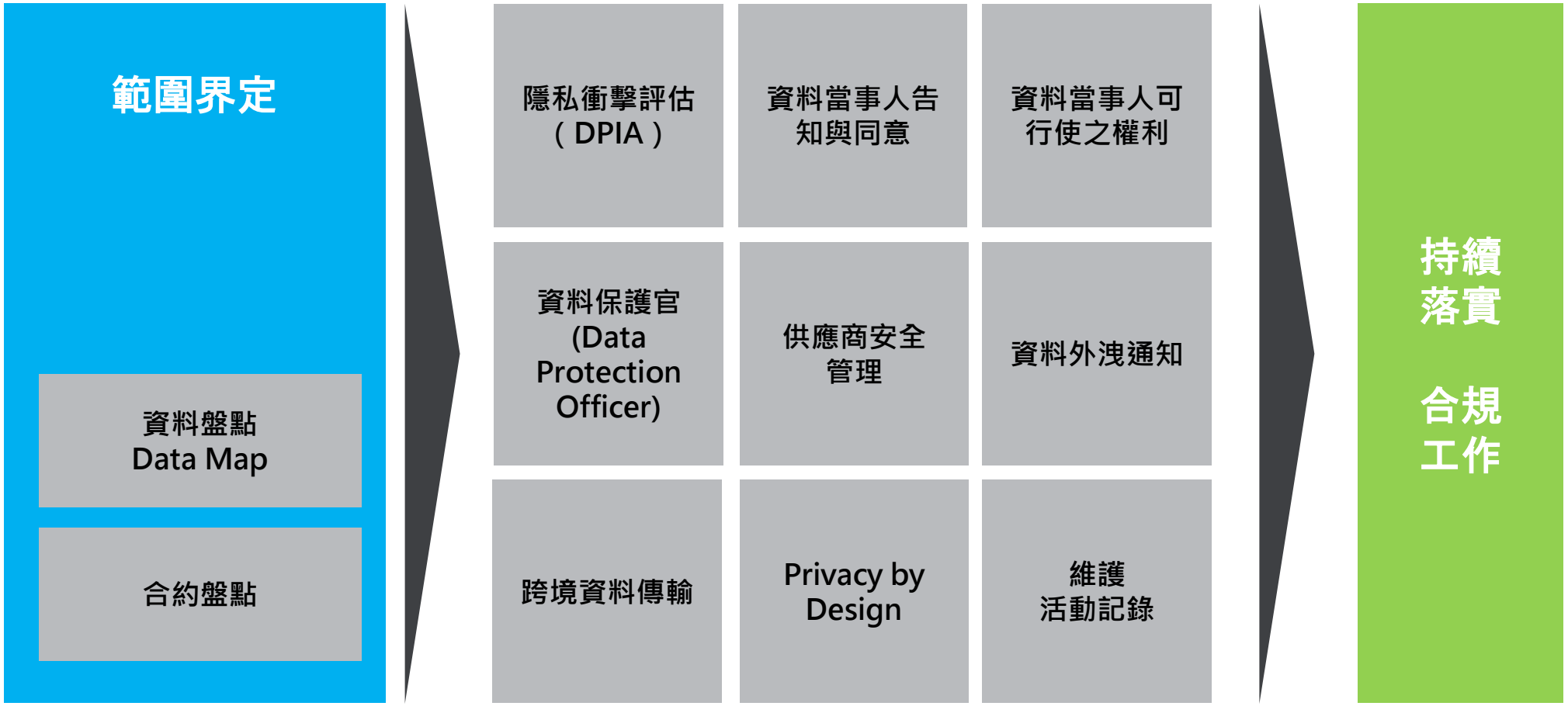
工作經歷
- Deloitte Risk Advisory (勤業眾信風險諮詢公司) – 執行副總, 總經理, 董事
- Ernst & Young LLP , U.S.A (先進運算實驗室) – 顧問, 專案經理
- 資訊工業策進會 – 專案經理, 經理
- 國立政治大學 資訊管理系 – 助教

學歷
- 國立政治大學法律研究所 - 法律碩士 (LL.M)
- University of Maryland, College Park - Ph.D Candidate
- 北京大學BiMBA (Non-Degree) Program
- University of Colorado, Boulder – Master of Science / M.B.A – Information Systems

公共事務
- 行政院資通安全會報 - 諮詢委員
- 經濟部技術處 - 科技專案審查委員
- 台北市政府 - 市政顧問 (網路與智慧城市類)
- 金管會檢查局 – 監理科技講座
- 經濟部工業局 - 行動APP 檢測制度諮詢委員
- 經濟部商業司 - 電子商務產業- 行政檢查委員
- 教育部高教司 – 跨域人才培育計畫諮詢委員/教學評鑑委員
- 法務部調查局 - 資訊安全與數位鑑識 – 諮詢委員

研究興趣與領域
- 資訊科技法律 (Cyber Law)
- 系統動力學 (System Dynamics) / 社會系統模擬
- 演算法與系統模擬 (Algorithm & system simulation)
- 資訊治理 (IT Governance)
- 資料庫逆向工程 (Data Base Reengineering)
- 風險治理與數據分析 (Risk Governance)
- 資訊系統安全/ 安全稽核與鑑識

個資保護稽核的標的：個人資料保護作業與控制落實重點



個人資料保護的落實與稽核 – 以資料當事人權利行使為核心

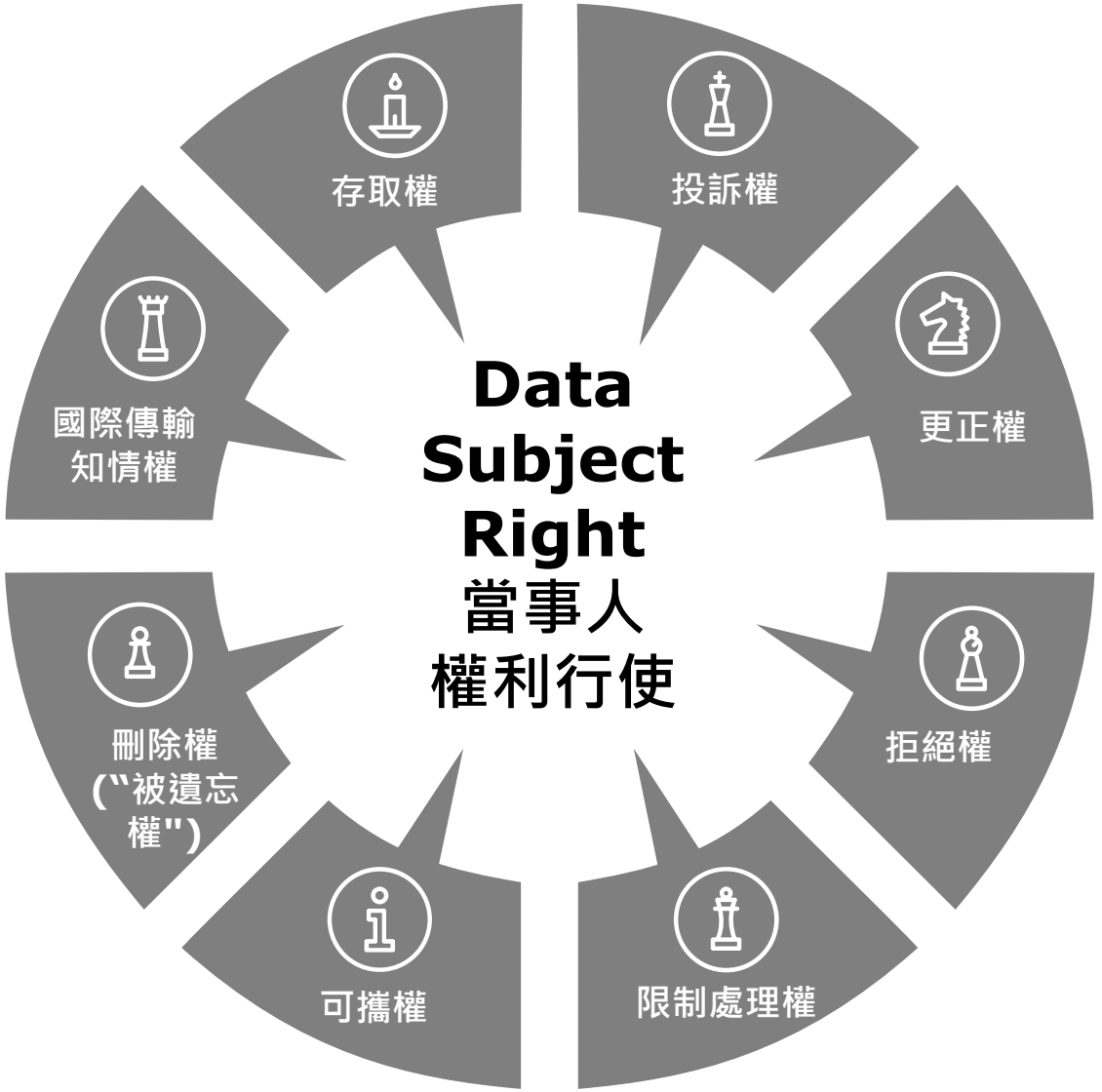
資料保護的侵權事件,每一類型的案例都是獨特的, 沒有通則

Right to be informed about all the personal you have on them (and ask for a copy).
有權知悉您所持有的其所有個人資訊（並請求獲得對應副本）。

Right to be informed about who you share their personal data with (and ask for a copy of agreements concluded with these recipients).
有權知悉從貴方獲得其個人資訊的各方（並請求獲得您與該等接收方簽訂之協議的副本）。

Right to ask you to delete their personal data.
有權請求您刪除其個人資訊。

Right to ask you to move their personal data to a third party.
有權請求您將個人資訊轉移到協力廠商。



Individuals have the right to be informed that they can issue a complaint with the regulator.
個人有權知悉其可向監管機構投訴。

Right to ask you to correct, complete or update their personal data.
有權請求您更正、補充或更新其個人資訊。

Right to object to you having access, storage and using their personal data.
有權拒絕您訪問、存儲及使用其個人資訊。

Right to ask you to suspend the access, storage or use of their personal data.
有權請求您暫時停止訪問、存儲或使用其個人資訊。

Privacy by Design與Privacy Engineering

積極主動，而非消極被動; 預防性，而非事後補救

預設隱私設計（PbD）方法的特點是主動而不是被動的措施。 預測並防止隱私事件發生。 “隱私設計”是事前的，而不是事後。

隱私以預設設置

隱私設計旨在通過確保個人資料在任何IT系統或業務流程中自動受到保護，從而提供最大程度的隱私。 個人不需要採取任何行動來保護他們的隱私 – 因為它是預設在系統中的。

將隱私嵌入到設計中

隱私嵌入到IT系統和業務流程的設計和體系結構中，且並不是作為附加，而是成為交付的核心功能。

全功能 – 整合，而非零和

隱私設計旨在“雙贏”的方式滿足所有法規遵循利益和目標。

點到點的安全性 – 完整的生命週期保護

預設隱私設計(PbD)在蒐集資訊的第一步之前即嵌入到系統中，從頭到尾貫穿整個資料生命週期。

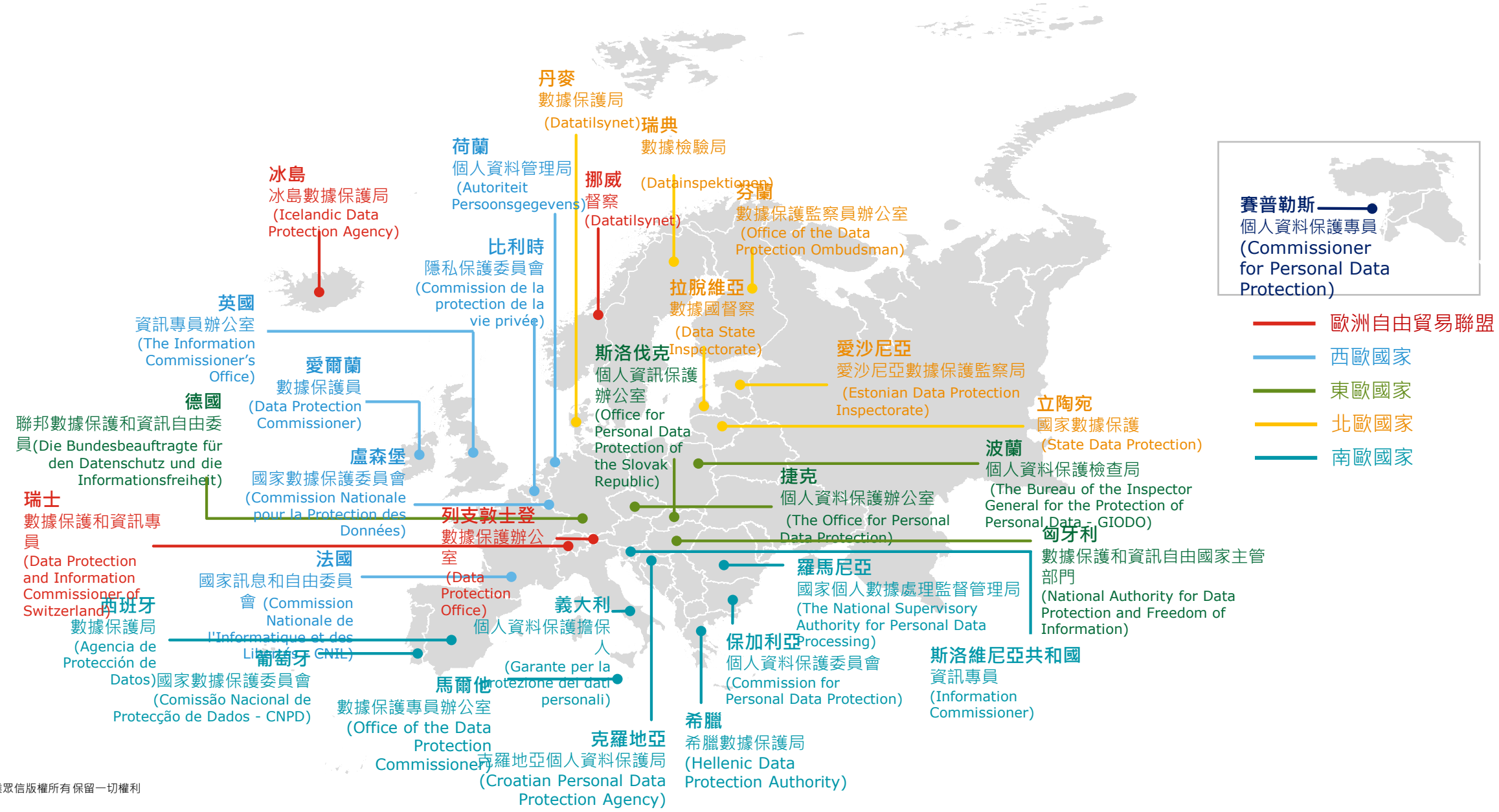
可見性和透明度 - 保持開放

“隱私設計”旨在向所有利害關係人保證，無論涉及到哪種業務流程或技術，實際上都是按照所述的承諾和目標進行運作的。

尊重使用者隱私 - 以使用者為中心

隱私設計需要建構人原和營運人員通過提供強力的隱私預設設置，適當的通知及人性化選項等措施來保持個人利益。

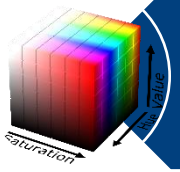
從資料流的角度觀察, 我國缺乏單一個人資料保護的事權機關



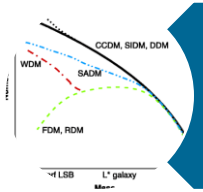
亟待推廣數據分析應用潮流下，個資去識別化有效性驗證實

藉由資料分析方法，客觀驗證去識別化後資料可能存在之風險

單一性風險驗證：檢驗去識別化後，加密符碼是否存在有一對一的情況，可能經由資料交叉比對破解加密規則



連結性風險驗證：檢驗去識別化後屬性組合是否具有一定數量以上無法區分，以避免透過資訊連結出個人特徵



可推測性風險驗證：檢驗去識別化後，一般及敏感屬性是否有某一組合存在小樣本情況，發生同質性攻擊機率高

資料可用性驗證：檢驗去識別化後資料分布是否接近原資料值分布，保留資料資訊及分析可用性

如何將法規需求轉變成為可執行的程序或工程技術, 有待完善

Privacy Engineering framework

Right of access (Art. 15)	Right to rectification (Art. 16)	Right to be forgotten (Art. 17)	Restriction of processing (Art. 18)
Right to data portability (Art. 20)	Profiling (Art. 22)	Privacy by design and default (Art. 25)	Security of processing (Art. 32)
Purpose limitation (Art. 5)	Data minimisation (Art. 5)	Accuracy (Art. 5)	Storage limitation (Art. 5)
Integrity and confidentiality (Art. 5)			

網路科技普及, Cybersecurity對個資保護的成敗影響既深也廣, 成本也遽增

Cloud and Big Data

ENISA has written a number of papers on Cloud Computing Security and recently focused on Big Data security.

Sub-topics:

- Cloud Security
- Big data

Critical Infrastructures and Services

The need to ensure ICT robustness against cyber-attacks is a key challenge at national and pan-European level.

Sub-topics:

- Critical Information Infrastructures
- Internet Infrastructure
- ICS SCADA
- Smart Grids
- Finance
- Health

CSIRT Services

An important aspect when establishing a CSIRT is to define its core services according to the available internal resources.

Sub-topics:

- Reactive Services
- Proactive Services
- Quality Management
- Community Projects

CSIRTs and communities

ENISA's work on cooperation between CSIRTS and other operational communities.

Sub-topics:

- Law Enforcement
- Finance
- ICS-SCADA
- Energy

CSIRTs in Europe

ENISA is at the heart of a pan-European collaboration network of CSIRTs.

Sub-topics:

- Glossary
- CSIRT Inventory
- CSIRT Capabilities
- CSIRT Cooperation

Cyber Crisis Management

ENISA pioneers the development of proper mechanisms and consistency for cyber incident and crisis management.

Sub-topics:

- EU-level Cyber Crisis Management
- National-level Cyber Crisis Management
- International Conferences
- Trainings

Cyber Exercises

ENISA is supporting and organising cyber exercises.

Sub-topics:

- Cyber Europe
- Cyber Exercises Platform
- Trainings and Studies
- Supporting Other Exercises

Cyber Security Education

ENISA is active in the area of education and awareness, using its knowledge to promote NIS skills.

Sub-topics:

- European Cyber Security Month
- EU Cyber Challenge
- NIS in Education

Data Protection

Privacy and data protection constitute core values of individuals and of democratic societies.

Sub-topics:

- Privacy by Design
- Privacy enhancing technologies
- Security of personal data
- Personal data breaches
- Online and mobile data protection

Incident Reporting

ENISA's work with Incident reporting and security regulation (Article 13a and Article 19).

Sub-topics:

- For Telcos
- For Trust Providers
- For Digital Service Providers (NIS Directive)

IoT and Smart Infrastructures

Smart Infrastructures rely on cyber-physical systems and IoT devices to enhance the quality of a service. Hence, they are exposed to cyber threats and need to be secured.

Sub-topics:

- Smart Cars
- Smart Homes
- Smart Airports
- Smart Cities

National Cyber Security Strategies

In a constantly changing cyber threats environment, EU Member States need to have flexible and dynamic cyber security strategies to meet new, global threats.

Sub-topics:

- National Cyber Security Strategies Guidelines & tools
- National Cyber Security Strategies (NCSSs) Map
- Public Private Partnerships (PPPs)
- Information Sharing and Analysis Centers (ISACs)

Standards and certification

ENISA supports the development of ICT security standards and certification frameworks in Europe.

Sub-topics:

Threat and Risk Management

ENISA threat and risk management provides an overview of threats, together with current and emerging risk and trends.

Sub-topics:

Trainings for Cyber Security Specialists

ENISA's Cyber Security Training material was introduced in 2008, and has grown continuously ever since.

Sub-topics:

Trust Services

Trust services are a key element in increasing European citizens' and businesses' confidence in electronic transactions.

Sub-topics:

- Security measures

稽核時，心中常存核心概念

存取控制

- 系統將記錄個人（使用者和IT人員）對所有個人資訊的存取權限
- 在可能的情況下，使用加密（和其他隱私增強技術（PET））來保護儲存的資訊，只有經過授權的使用者才能查閱
- 存取控制將以最高的程度級別被預設到系統中。定其自動檢視存取權限

通知要求

- 該系統將以簡潔，易懂且易於存取的格式提供，使用清晰和通俗的語言在蒐集時提供通知
- 必須保留記錄，證明何時通知相關的資料當事人

管理個人隱私權

- 確保功能上能回應個人要求，包括資料可移植性流程。考量再識別與間接識別的可能性

供應商要求

- 只有最小數量的個人資訊會被轉移給任何第三方（並且僅用於通知目的）。 第三方必須具有適當的控制

同意要求

- 在必要時，必須收到並記錄正式的明確同意，需要可選擇加入
- 獲取適當的原始資料，以確保個人資料得到公平處理
- 確保處理個人撤回同意的流程

資料蒐集

- 只蒐集系統運行絕對需要的最少量個人資訊。 所有蒐集到的資料都將受到檢視
- 在可能的情況下，個人資訊將去識別化（從個人資訊中刪除標識符號）。 並只能使用匿名資訊進行測試

資料品質

- 為每個需要資訊的目的設置“檢查”日期
- 如果“檢查”日期超過了規定的時間，而沒有經過審查和簽署，則自動處理個人資訊
- 提供資料當事人人提供清晰，簡單，有效的流程

同意要求

- 必要時會收到並記錄正式的同意書。在大多數情況下，需要可選擇加入
- 在您的聯繫記錄中獲取適當的原始資料，以確保個人資料得到公平，合法、透明的處理
- 確保處理個人撤回同意的流程。個人應可輕鬆地取消的同意，確保系統/流程能適當管理撤銷的結果

跨境傳輸

- 在可能的情況下限制跨國界的個人資訊傳輸（包括從本國管轄範圍以外的存取）。確保控制措施可以得到落實，以符管理法律和安全要求。

資料保留

- 系統中的所有個人資訊將設有一個保存政策，並預設到系統中，以便在保留期限屆滿後刪除該資料。

Deloitte.

勤業眾信

About Deloitte
Deloitte 泛指Deloitte Touche Tohmatsu Limited(即根據英國法律組成的私人擔保有限公司，簡稱"DTTL")，以及其一家或多家會員所。每一個會員所均為具有獨立法律地位之法律實體。Deloitte("DTTL")並不向客戶提供服務。請參閱 www.deloitte.com/about 了解更多有關Deloitte及其會員所。

Deloitte為各行各業的上市及非上市提供審計、稅務、風險諮詢、財務顧問、管理顧問及其他相關服務。Fortune Global 500大中，超過80%的企業皆由Deloitte遍及全球逾150個國家的會員所，以世界級優質專業服務，為客戶提供因應複雜商業挑戰中所需的卓越見解。如欲進一步了解Deloitte約245,000名專業人士如何致力於”因我不同，惟有更好”的卓越典範，歡迎瀏覽我們的Facebook、LinkedIn、Twitter專頁。

About Deloitte Taiwan
勤業眾信(Deloitte & Touche)係指Deloitte Touche Tohmatsu Limited(“DTTL”)之會員，其成員包括勤業眾信聯合會計師事務所、勤業眾信管理顧問股份有限公司、勤業眾信財稅顧問股份有限公司、勤業眾信風險管理諮詢股份有限公司、德勤財務顧問股份有限公司、德勤不動產顧問股份有限公司、及德勤商務法律事務所。

勤業眾信以卓越的客戶服務、優秀的人才、完善的訓練及嚴謹的查核於業界享有良好聲譽。透過Deloitte資源整合，提供客戶全球化的服務，包括赴海外上市或籌集資金、海外企業回台掛牌、中國大陸及東協投資等。