

如何讓企業能夠充份了解並及時準備符合GDPR的要求，便成了一個重要的課題，以避免因GDPR帶來的營運風險。

## GDPR 的合規展現與PIMS國際標準

# GDPR倒數計時

文／梁日誠

**歐**洲隱私權法律——一般資料保護規定(General Data Protection Regulation, GDPR)，即將於2018年5月25日生效。依此規定，企業若未遵循該法規要求，主管機關得進行調查，最重可裁處企業「2,000萬歐元」或該年度「全球營業額4%」的罰鍰（取其高者），本文說明企業展現GDPR合規性之幾項可行途徑與相關PIMS(personal information management system)國際標準。

本文提及的國際標準所指為經各國投票同意而公告發行的ISO國際標準(International Standard)，和坊間誤以為國外標準就是國際標準的認知是不同的，國外標準或其它國家的國家標準（如加拿大CAN、英國BS、德國DIN等）在國際上並不被稱為國際標準。

### GDPR適用對象

依 GDPR Article 3 Territorial

scope 規範，GDPR適用對象說明如下：

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
- 台灣的銀行在歐洲設立的分行，無論其蒐集的個資是在歐盟境內處理或境外（如台灣）處理，都要受到規範。
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
  - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in

the Union; or

- 在臺灣設立的線上訂票或購物網站，提供歐盟境內自然人訂票或訂購商品；或是臺灣將電子產品銷售至歐洲，並提供產品註冊及相關售後服務者；或是提供付費/或免費的 IOS/ Android App，只要會蒐集或處理歐盟境內自然人相關個人資料。

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

- facebook蒐集歐盟境內自然人相關社交行為；線上支付系統如提供歐盟境內自然人使用之相關支付管理；或是使用cookie來紀錄使用者瀏覽行為之網站…等，只要會蒐集歐盟境內自然人相關行為者。

如表1示意，此法規不僅適用在歐盟境內設立公司的企業，即使未在歐盟設立公司，只要會蒐集或處理到歐盟境內自然人相關個人資料（如姓名、地址、GPS位置、通訊紀錄等），都要受到規範，而且要依 Article 27 在歐盟指派一代表。惟表1右下，歐盟自然人不在歐盟時（如德國居民派駐在台灣工作）的個人資料蒐集或處理是否受到GDPR規範，目前仍屬灰色地帶。

## 展現GDPR合規的方式

GDPR在以下Articles提及以認證體制可展現對GDPR的合規

表1 GDPR適用對象的識別。

控制者或處理者 所在地 當事人所在地	歐盟境內	歐盟境外
歐盟境內	Article 3.1	Article 3.2
歐盟境外	Article 3.1	Article 3.2

控制者: Controller 處理者: Processor 當事人: Data Subject

性：

- Article 24 Responsibility of the controller
- Article 25 Data protection by design and by default
- Article 28 Processor
- Article 32 Security of processing
- Article 35 Data protection impact assessment
- Article 46 Transfers subject to appropriate safeguards
- Article 83 General conditions for imposing administrative fines

GDPR 第四章節 (CHAPTER IV) Section 5 Codes of conduct and certification 規範了展現GDPR合規的兩種方式：行為準則(Codes of conduct)及驗證(Certification)。

- 第一種方式：採用行為準則 (Codes of Conduct, CoC) 應依循 GDPR Article 40及41 規範。可由歐盟會員國內的協會或其

它團體起草行為準則（包含監督機制），再由監管機構核准；如果與多個歐盟會員國相關的協會或其它團體，則要將行為準則提交給歐盟資料保護委員會 (European Data Protection Board, EDPB)。後續則由監管機構認證的監督機構對「控制者 (Controller)或處理者(Processor)」進行監督工作，如圖1。

- 實際案例：Amazon採用CISPE（歐洲雲端基礎設施服務供應商聯盟）行為準則(CoC)來展現其雲端基礎設施依照歐洲GDPR使用適當的資料保護標準來保護其資料，目前此聯盟所提出之行為準則是以IaaS供應商為主，惟 Article 29 Working Party（之後將成為 European Data Protection Board, EDPB）已正式回函CISPE指出其CoC尚待增補之處。

2. 第二種方式：採用驗證 (Certification)應依循 GDPR Article 42及43 規範。

各會員國的監管機構以(EC) No 765/2008 規定治理認證機構，認證機構以 ISO 17065 及附加要求治理驗證機構，最長五年；驗證機構(如CIS)對「控制者或處理者」實施驗證作業，或可由歐盟資料保護委員會或監管機構核發資料保護驗證，印章或標章，最長3年，如圖2。惟歐盟有關GDPR驗證機構認證的實作指引於2018年3月30日前仍位於公開徵求意見的階段。

### 資料保護驗證 (certification)、印章(seals)或標章(marks)機制

針對目前已發展的幾個存在於歐盟內的機制舉例說明如下：

- 歐盟隱私印章(European Privacy Seal, EuroPriSe)在整個歐盟地區

提供 IT-based 產品與服務的驗證。但仍需要監管機構或認證機構或歐盟資料保護委員會認證或同意。值得注意的是，在EuroPriSe的驗證方案中，也認可目前的 PIMS-Specific 驗證（如ISO27018）與之後的 ISO27552 驗證做為其驗證方案中的一部份。

- 法國資料保護機構的「Label CNIL」隱私驗證方案(privacy certification scheme)。但仍需要歐盟資料保護委員會認證或同意。
- BSI在英國或台灣推動的BS10012 標準與驗證。仍需要監管機構、認證機構或歐盟資料保護委員會認證或同意。須留意的是EU已於2018年1月正式發函公告，於2019年3月30日後，脫歐後的英國後將成為第三國(third country)，如同美國、

加拿大與台灣之於GDPR的關係，第三國的個資標準被EU接受的可能性極低。惟ISO會員國均可等同採用ISO標準而成為其國家標準，如，BS ISO29151、BS ISO29134、BS ISO27018、BS ISO27001 等PIMS與ISMS的ISO標準也已成爲英國國家標準，對於脫歐後的各英國組織而言，仍可採用其它歐盟國家所認可的ISO標準做為GDPR的合規展現，惟日後或將須尋求經EU內的認證機構所認證的驗證機構進行驗證方足以被接受符合GDPR要求。

- Privacy Information Management System (PIMS) 相關標準，由ISO根據 ISO27001 的現有認證方案發布，已經存在於認證機構認證之下，且歐盟會員國俱爲ISO會員國，可等同採用ISO標準，如ISO29151、ISO27018、ISO29134、ISO27552(發展中)等。對於EU外的眾多第三國，因亦爲ISO會員國，若EU的共通驗證(common certification)最終採用ISO的標準，相信俱爲國際間所樂見。

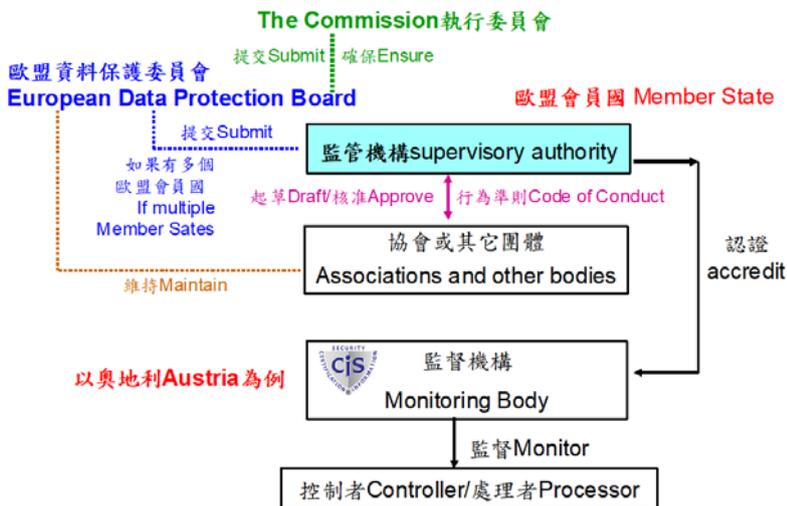


圖1 GDPR行為準則的認證體制關係圖：Article 40及41。

### ISO發展的個資保護驗證

基於ISO國際標準的個資管理系統PIMS，如圖2，個資管理系統之驗證機制，是以 ISO 27001 延伸驗證的方式實施，ISO 27001 延伸驗證除了補強原先 ISO 27001+ISO27002 的不足

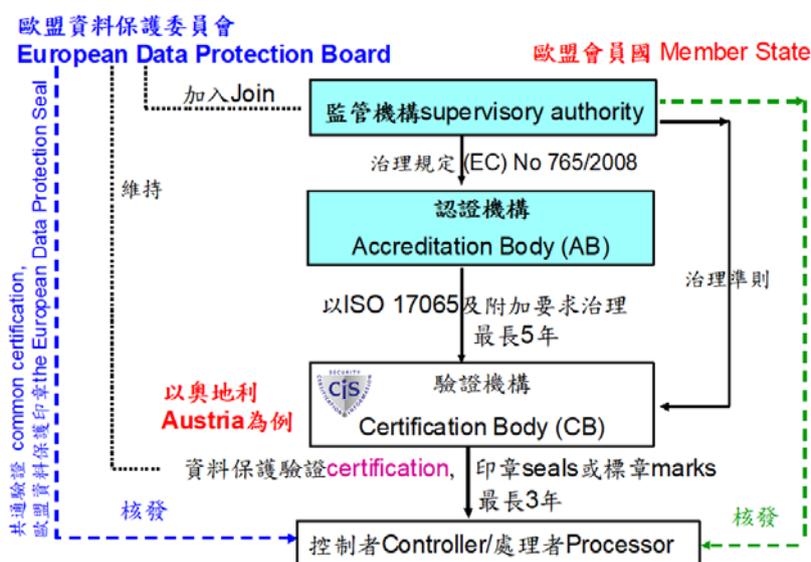


圖2 GDPR驗證的認證體制關係圖：Article 42及43。

外，亦可有效加強組織對於資訊安全實作的深度及廣度。ISO 27001延伸驗證依據 ISO 27009 Sector-specific application of ISO/IEC 27001-Requirements 特定領域應用 ISO/IEC 27001 的要求，個資管理系統之驗證即為個資的特定領域 PIMS-Specific 的延伸驗證。

目前國際各大企業 Microsoft、Amazon、Dropbox、IBM、Google 及中國地區的百度、企業微信、騰訊、平安科技等，均已採用 ISO 27018 (based on ISO27001) 做為 PIMS 個資保護延伸驗證 (based on ISO27009)。

在國際上，能夠核發具備認證機構認證的 PIMS ISO27018 證書的驗證機構為數不多，CIS/TCIC 就是其一。筆者任職的環奧國際驗證有限公司 (TCIC) 總部位在加拿大不列顛哥倫比亞省 (British

Columbia, Canada)；於亞洲地區設有分支機構並建立了當地的服務團隊，歐洲總部 (CIS) 位於奧地利維也納 (Vienna)，亦為一第三方管理系統與人員驗證機構。TCIC 與 CIS 互為授權機構，素以第三方獨立公正的驗證與評鑑服務為全球市場所認可。CIS/TCIC 專注於資訊安全 (ISMS)、服務管理 (SMS)、營運持續 (BCMS)、個資保護 (PIMS) 等管理系統驗證稽核，車聯網稽核 (MirrorLink Audit) 與教育訓練服務，並且核發了台灣第一張 ISO27018 證書與第一張 ISO29151 證書。GDPR 認證體制正式上路後，CIS 為 EU 內經認證的驗證機構，TCIC 為 CIS 於非 EU 國家的授權機構，一併納入 EU 認證機構的認證範圍內，可提供全球化的 GDPR 驗證服務。CoC (含監控) 亦將是 CIS 的服務項目之一。

## 如何從 ISMS 到 PIMS

對於已經熟悉 ISMS/ISO27001 的組織而言，建立以 ISO 標準為依據的 PIMS 是最有效率的選擇。目前尚無建立 ISMS 的組織，可以選擇同時建立 ISMS 與 PIMS 並通過驗證。ISMS 與 PIMS 的驗證相關標準列舉如下，各標準的交互關係如圖 4。

- ISMS :
  - Information Security Management System
  - 資訊安全管理系統
  - 驗證標準：ISO/CNS27001
- PIMS :
  - Privacy Information Management System
  - 個資管理系統
  - 驗證標準：ISO29151 & ISO/CNS27018 (適用於對外服務)，包括 ISO29134 以及 based on ISO/CNS27001、ISO 27009 與 ISO/CNS29100。

## GDPR 認證體制對 GDPR 的合規展現案例

採用行為準則 (Codes of conduct) 或驗證 (Certification) 雖為志願性，但 GDPR 中，如「Article 25 Data Protection by design and by default」及「Article 35 Data protection impact assessment」為必須執行的要求且可透過上述機制展現其合規性。其對應的 ISO 國際標準以下以兩個案例說明：

- 案例一、GDPR Article 25 Data

protection by design and by default  
什麼是「Data protection 'by design' and 'by default」？歐盟的說明範例如下：

- Data protection by design

使用擬匿名化(pseudonymization)，用人工識別符代替個人可識別資訊和加密，將訊息編碼，只有被授權的人才能閱讀。

- Data protection by default

社交媒體平台宜鼓勵用戶的隱私基本設置限制用戶個人資料的可訪問性，以在預設的情況下不會讓所有的人可以訪問。

ISO於2017年發展出全球首個適用於所有類型組織的個資保護控制措施的國際標準「ISO 29151：個人可識別資訊保護實務」(Code of practice for personally identifiable information protection)，包括了37項依 ISO 27002:2013 控制措施擴充實作指引，以及27項依 ISO 29100 之隱私原則新增的控制措施，依其 Clause 4.4 的標準內容，可用來展現 Privacy (Data protection) by design，且 ISO 29151 可進行PIMS驗證。

- 案例二、GDPR Article 35 資料保護衝擊評鑑(Data protection impact assessment)

ISO於2017年發展出全球首個適用於一般組織的隱私衝擊評鑑的國際標準「ISO 29134：隱私衝擊評鑑指引(Guidelines for privacy impact assessment)」，此標準定義21個具體的步驟，可有效指引正

確且有效的實施資料保護衝擊評鑑。

而且此一標準亦獲得歐盟執行委員會(EC)採用為GDPR DPIA方法之一。

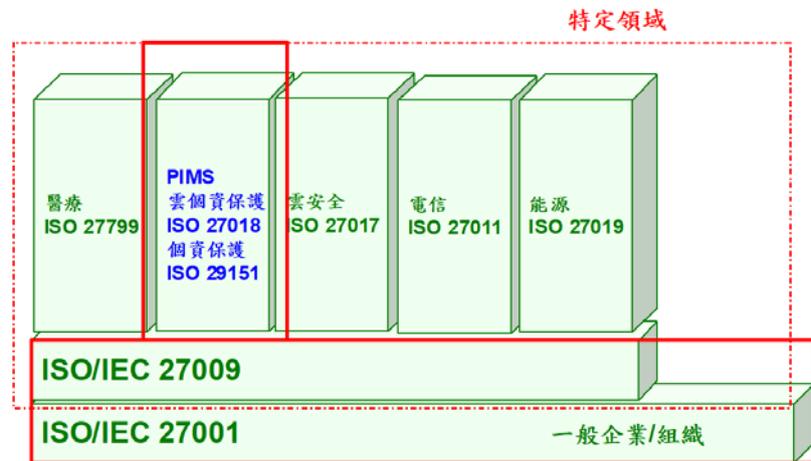
### ISO組織對應GDPR的標準—ISO/IEC 27552(正發展中)

為因應GDPR，法國資料保護機構(DPA)向ISO提議發展 ISO/IEC 27552。目前 ISO 27552 的現階段版本為Committee Draft(CD)，由德國的DIN擔任秘書處協調整體發展工作。此一標準包括PIMS有關於個資控制者或處理者的特定要求(requirements)與實作指引(guidance)並包含適用於個資控制者或處理者的控制措施，與GDPR的對應關係，與 ISO29100、ISO27018、ISO29151 的對應關係。其中附錄C(Annex C)為 ISO 27552 與GDPR的對應關係，提供 ISO 27552 對

GDPR的最佳且直接的合規展現，若PIMS現在使用 ISO29151 或 ISO27018 標準，ISO組織也提供了一個對應表，可以由 ISO29151/ISO27018 順利轉換到 ISO27552。值得注意的是，目前的EU國家，如德國DIN及英國BSI均在ISO27552 發展階段就成立專案支持，可在ISO27552一經公布即在最短時間內等同採用，可見此一標準受重視的程度。

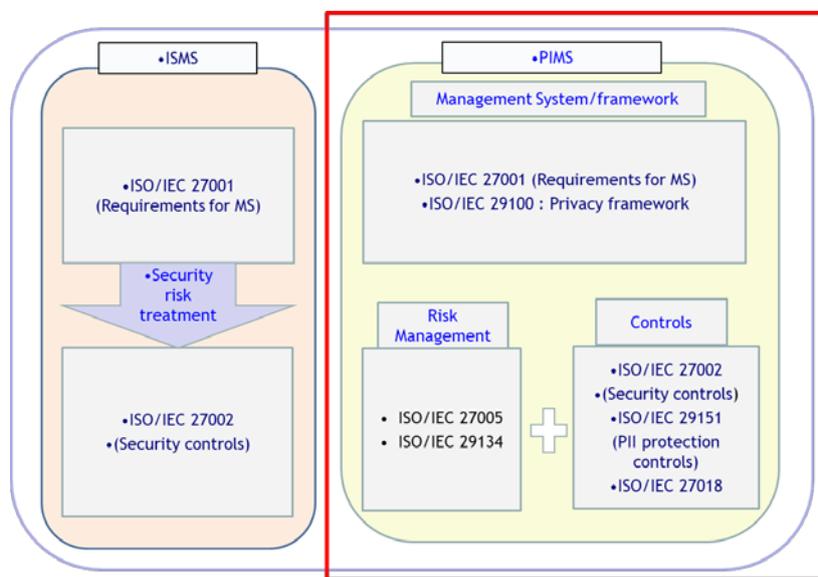
### 第三國(third country)應對GDPR施行的參考方式

GDPR要求若要傳輸歐洲居民個資至第三國(third country)或國際組織(international organization)前均須獲得同意，對此要求，第三國可與歐盟協商是否其國家符合歐盟認可的安全保護足夠國家，目前歐盟認可了 安道爾、阿根廷、加拿大(商業組織)、法羅群島、根西



註：ISO仍持續發展資安與個資保護標準(如，ISO 27552 Enhancement to ISO/IEC 27001 for privacy management – Requirements) 來因應世界潮流(如，GDPR)。

圖3 基於ISO國際標準的個資管理系統PIMS。



Source: ISO及TCIC綜整

圖4 從ISMS到PIMS。

島、以色列、馬恩島、澤西島、紐西蘭、瑞士、烏拉圭和美國（僅限於隱私保護框架）提供足夠的安全保護。歐盟並公佈了正在洽談足夠的安全保護的國家，如日本與南韓，台灣尚未見於歐盟公告中。若企業所在的第三國未被認可成為足夠的安全保護的第三國，企業就必須尋求其它方法的同意，如驗證、CoC(含監控)、Binding Corporate Rules(BCR)等。

如何讓企業能夠充份了解並及時準備符合GDPR的要求，便成了一個重要的課題，以避免因GDPR帶來的營運風險。以加拿大為例，筆者在加拿大受邀擔任國家層級 Advisory Committee on GDPR（GDPR諮詢委員會）委員，除了由國家層面與歐盟進行足夠的安全保護的第三國協商並取得歐盟認可外，並

由各個與GDPR相關利害團體組成GDPR諮詢委員會並由加拿大標準委員會(Standards Council of Canada, SCC)支持，任務在協助加拿大企業準備面對GDPR並掌控風險，同時也尋求可能的商機與創新機會。

總合而言，無論是要符合歐盟的GDPR或其它地區的個資保護法規，ISO均已規劃或準備好對應的國際標準，採用國際互通的PIMS ISO標準是不二選擇。筆者有感於國內對於PIMS標準認知的異象，如，仍誤以為使用他國標準為展現符合台灣個資法規的正途、ISO的PIMS標準已經公告仍被引導進行他國標準的轉版升級而錯失將PIMS轉換為ISO標準的機會而導致錯誤的投資，加上GDPR施行在即，PIMS國家標準化(CNS)的工作刻不容緩，已整合加拿大

標準協會(CSA)與國家標準技術專家與審查委員進行 CNS29151 與 CNS29134 的國家標準的建議與起草工作，相信不久的將來台灣各組織將可有中文文化的PIMS國家標準可以閱讀及採用，不論是展現對國內個資法規的合規性或使用 ISO/CNS29151 與 ISO/CNS29134 做為GDPR的合規性展現，都更加容易。

CIO

### 梁日誠 Daniel Liang

1. TCIC環奧國際驗證公司 全球營運總經理/稽核師/講師
2. 加拿大標準委員會 SCC Advisory Committee on GDPR委員
3. Email: [daniel@mail.tcicgroup.com](mailto:daniel@mail.tcicgroup.com)