# 資安長的新重擔：資料主權法規遵從

## 目前已有超過一百個國家要求其公民資料必須要在其境內儲存或處理，為資料保護帶來全新挑戰。

文／Christopher Burgess　譯／柳百郁

你的個人資訊，其實就是資料主權的核心議題。你的資訊放在那裡？誰在存取你的資訊？你能否控制資料放置在每個國家的資訊位置，或是政府是否有權存取與控制你的個人資料？

甲骨文公司（Oracle）對資料主權管制的觀察是，跨國界及公有雲邊界的資料呈現出有目共睹的驚人指數型成長，已有超過一百個國家通過相關法案。尤其是對那些客戶群或數位基礎架構橫跨政治邊界的那些企業而言，並沒有一體適用的規則，而這成為企業資安長（CISO）的難題。

在2021年8月所發表的一篇論文中，美國喬治華盛頓大學（George Washington University）教授 Susan Ariel Aaronson 抨擊，在數位主權的面具下，「政府想方設法規範個人資料的商業用途，但卻沒有實施明確規則來管理政府單位對個人資料的使用。」

在2020年的歐盟議會 EPRS Ideas Paper 報告中，歐盟將數位主權形容為「歐洲各國在數位世界裡獨立行動的能力，且應從保護機制與攻擊工具兩個層面進行理解，才能促進數位革新（包括與非歐盟夥伴的合作）。」

如同DocPro執行長 Kim Chan 所指出，歐盟的通用資料保護規則（GDPR）有效地推動了一場巨變，其中涉及的不限於以歐盟為主的企業。GDPR成為歐盟規章，世界各地企業無不爭先恐後地遵循它。因為GDPR不僅適用於歐盟內部，亦適用於提供貨物與服務，以及蒐集與處理歐盟客戶資料的企業組織。

保障公民資料安全是普遍共識。非洲聯盟正致力於統一通用資料系統的發展。目標是「管控整個非洲大陸不斷增生的資料產出及使用，同時建立安全並值得信任的數位環境，支援可持續且含括一切的非洲數位經濟與社會體系發展。」

國際選舉制度基金會（IFES）資深顧問 Stephen Boyce 憶及IFES的經驗，由於該非營利組織在超過二十個國家設有辦公室，因此認為遵循所有國家的資料主權法將是一大挑戰。他認為需要更懂法律、GDPR與突發的一次性行為的人為此作出解釋，意即「我們的團隊必須重新開始思考它對營運的影響。」

對所有資安長與資訊安全服務代管廠商（MSSP）而言，迫在眉睫的問題是必須能回答：「資料在那裡？」這個關鍵問題。

### 避免侵犯資料主權

將資料存放到雲端平臺的企業組織必須體認到，並非所有廠商都打算採取相同方式；同時企業還必須作好盡職調查（due diligence），確認能避開將資料存放在實施資料主權法的地區。FindPeopleFast公司的 Daniela Sawyer 談及他親身體驗，發現想要查核資料是否只存放在於被允許的地點，是有一定難度的。這意謂著要求雲端平臺使用者必須信任他的雲端供應商，對於其伺服器主機代管位置全然坦誠又公開，並嚴格依循服務等級協議

(SLA)。

事實上，不是只有小公司可能會出問題。2021年5月，歐盟的歐洲資料保護監督機構，對歐盟中有多少機構使用AWS與Azure展開調查，要求供應商必須回應該平臺是否有充分地在保護使用者隱私。

## 為維護資料主權，企業營運開支預期將會增加

企業營運費用會受到維護資料主權的影響。ProPrivacy公司的Attila Tomaschek 說明：「企業會產生額外的持續性支出，包括在網路安全最佳實作方面的持續性員工訓練、對新技術與網路監控工具的投資，以及因此衍生出來的附帶相關人員，例如資料保護主管、法規遵從主管，或其他專職於保障企業資料安全與遵循資料保護法的人員等。」

Tauria公司執行長 Jesse David The 在談到該公司在因應GDPR過程的經驗時，也分享了類似觀點：「我們必須出示特定資料軌跡，解釋如何取得某人的聯絡資訊。他們有權要求父公司的系統忘掉他的資訊；而我們也必須有確切許可，才能對他們傳送行銷電子郵件。資料存放在我們的封閉環境（walled garden）之內，不能與任何夥伴分享。反之，除非客戶允許，合作夥伴也不能與我們分享客戶聯絡資訊。」

The指出，為了遵守法規而導致該公司營運費用上升，促使他們決定雇用「能夠協助我們確保CDPR合規性的資訊長」，同時也提醒小型企業要估算，為了遵守法規得耗用多少預算才夠。

## 資訊安全觀念（Infosec）必須進化

BreachRx公司執行長 Anderson Lunsford 提到，隨著保險公司被要求必須近乎即時通知使用者資料外洩或危害的發生，讓資料外洩通知需求發生改變。如果保險公司達不到這項要求，無疑是讓自己陷於承保承諾範圍的危機中。Lunsford更發現，有些資訊安全專家對應變計畫的規畫，多半是紙上談兵。太多企業並未實作這些情景的場景綱要，也沒有納入各種隱私法規的要求。

Lunsford指出了一個對資料外洩事件反應的特別觀察角度，尤其是在對企業施加行政處罰的狀況下。他認為這些被處罰的企業，多半不是資料外洩情況最嚴重的，而是沒有將應變工作處理好的。監管單位對此，也直言不諱表達他們的觀點。資訊安全與隱私產業普遍的認知，是所有企業組織都會發生意外；不是會不會發生，而是何時發生的問題。監管單位與客戶期望的是企業要為這個無法避免的狀況預先做好準備，並且能夠即時且適切地進行回應。

企業只能眼睜睜看著罰單送到眼前，而且有些對企業而言相當嚴苛。法律服務公司Morrison & Foerster（MoFo）在之前的 Privacy Minute 期刊當中，分享了俄羅斯境內外企業，收到要求企業確認他們將俄羅斯公民個人資料儲存在俄羅斯境內的狀況；Google的俄羅斯經驗值得借鏡。七月底，因為該美國科技巨擘拒絕將其使用者個人資料本土化在俄羅斯境內，因此莫斯科法院對Google處以三百萬盧布罰金（折合約$40,750美元）。

在印度，信用卡公司顯然發現對印度資料隱私法規難以適從；萬事達卡（MasterCard）是最近一個據稱違法，而在印度被禁止開發新客戶的企業。在MasterCard之前，則是美國運通（American Express）與大來卡（Diners Club）受到處罰，印度儲備銀行（RBI）無限期禁止這三家公司在印度國內市場發行新的信用卡或簽帳金融卡（debit card）。RBI則聲稱這幾家公司違反了印度的資料儲存法規。

TAG Cyber 公司研發與諮詢部門副總裁 Katie Teitler 表示：「由於全球各國對資料主權法的相異性與多樣性，迫使我們不得不更透徹檢視資料流向。但即便如此，到現在仍沒有一套簡單流程，能夠讓大型企業達到資料的充分能見度與監控的目標。市場上逐漸出現更新穎的工具協助達成此目標，但至少在可見的未來，企業還是得耗費許多時間與金錢在法規遵從上。」

可以想見的是，從長期角度來看，企業資安長與資訊安全團隊會面對大量且繁重的相關法規遵從工作。