跨國組織資料保護機制的遵循查核
Auditing Global Compliance of Data Protection Mechanisms

作者: **Dirk Lehmann, CISA, GCIA,**is director of IT audit at Siemens AG and has more than 16 years of experience in IT. Previously, he was manager of information security of the Siemens AG's corporate IT department and led the Siemens computer emergency response team branch in the US.

Frank van Vonderen, CISA, CGEIT, MSIT, is managing consultant at Dutch consulting company Verdonck, Klooster & Associates and has more than 13 years of experience in IT advisory and auditing for several multinationals. Previously, he worked at Siemens AG as manager of IT audit, and he has published several articles on IT sourcing, operations and security in various Dutch magazines. He can be reached at frank.vanvonderen@vka.nl.

譯者: 孫嘉明, CISA, ISO27001 LA, ACDA 雲林科技大學會計系 助理教授

在今日社會中，對於個人資料的保護日益受到關注。[1] 由於新興科技及社交網路的普及，大量個資更容易被多方取得且散播多處。因此，各國紛紛制訂或修正個資保護的法令以增加保護的效力。

然而，各國對於個資保護的範圍及規範卻有很大差異，使得對於跨國的全球化組織而言，同時遵守不同的各國法令成為一項挑戰。

全球法令遵循稽核即因以下因素而受到重視：

- 全球各地法令制定單位對於個資關注日趨增加；
- 國際化組織多次個資外洩事件的發生；
- 避免因法令遵循未落實事件導致財務及評價風險。

遵循目標決定稽核方向

全球化營運的企業大多採取以下兩種不同做法以滿足資料保護法令的要求：[2]

- 依據各國的規範各自執行處理：該做法雖然在各國法令初頒佈及查核期間，容易遵循執行；也可能造成相同的問題在不同的國家重覆發生。
- 採用全球一致的資料保護政策：以全球組織共同遵守的政策針對各種可能的缺失進行預防、偵測及回應。例如：資訊系統專案[3]中對於所收集的資料，便採用一致的保護措施，而不需要個別考量各國不同資料提供者對於資料保護的要求。該做法較容易確認政策的有效性，避免資料外洩事件。

不論採取那種做法，應當理解的是：沒有組織可以完全防止資料外洩事件，因為員工總是會犯錯的。例如：不小心將個資檔案寄給無關的人員或是遺失存有重要個資的隨身碟或磁帶。

評估組織是可否有效減少系統上的弱點至可以接受的程度，在於是否事前由管理階層於風險評估過程中，確認組織可接受的風險胃納(risk appetite)。組織所制訂的風險水準、風險胃納及風險圖像(risk profile)將會影響所採取的風險回應行動。

對於資料保護而言，風險水準、風險胃納及風險圖像受到以下因素的影響：[4]

1. **各產業的作業規範：**各項作業活動均需要遵守該產業的規範，例如：金融及醫療產業便比其他產業更要受到高度的監理與嚴格的規範。

2. **特定國家的嚴格法令要求：**某些國家的資料保護法令較其他國家更為嚴格。例如：德國即有很嚴謹的執行架構，而美國企業則是較容易因為民眾的控訴而導致重大財務損失。[5]
3. **個人資料與組織業務的攸關性：**如果個資處理為企業的核心業務，例如：代管人事應用系統資料，將比一般顧客的基本資料庫更容易受到資料外洩事件的衝擊。
4. **個人資料儲存的資料量：**所儲存的資料庫越大，越容易因為意外而導致外洩。而個資保管的資料量越多，因外洩而導致的罰鍰也將隨之昇高。[6]

法令遵循稽核

當企業決定採用依國家個別規範進行個資保護遵循時，其稽核重點將在於各個國家個資保護法令的要求項目。常見的資料保護法令主題如下：[7]

- 資料特徵及範圍，例如使用目的限制、使用範圍、以及資料保存。
- 個人資料的收集及儲存需清楚告知其個資對象。
- 個人有權被告知並詢問何種資訊被蒐集及所儲存的位置。
- 協助企業處理個人資料的第三方廠商所應負起的責任。
- 資料外洩時所應進行的告知程序

稽核活動及問項應當特別針對法令要求設計，以確保組織是否落實遵循。部分法令有可能特別指出那些控制要求需要遵循[8]，例如：是否進行資料分類及制訂資料保護政策。在歐洲，有關隱私權的法令遵循，更是提供了各式的資料可供資料人員進行稽核活動的準備。[9]

稽核資料保護制度的有效性

稽核資料保護制度的目的在於瞭解組織是否能夠有效地處理資料保護管理制度上的問題。但是什麼是資料保護制度呢？內部稽核協會指出資料保護制度主要包含以下活動：[10]

- **制度與程序：**組織應當建立防止員工及相關人員違反資料保護法令的遵循制度及作業程序。
- **高階主管的權責：**組織應在制度及程序中明確指出負起遵循監督的相關主管人員。
- **遴選可信任的人員：**組織應在人員遴選過程中，善盡管理人責任，小心避免給予有犯罪傾向的人員過高的權限。
- **溝通程序：**組織應當有效地將其標準及程序傳達給其員工及相關人員。
- **遵循監督及稽核：**組織應當採取適當的程序以確保對其標準的遵循。
- **一致性的維持：**組織應當建立明確的獎懲制度，使得違反標準的員工受到懲處。
- **對違規事件的回應及預防：**當發生違規事件時，組織是否採取合理的程序予以回應並預防相似事件的再次發生，包括程序的修正以加強法令遵循的預防與偵測。

檢查上述機制是否存在且有效運作，為資料保護制度稽核的主要查核項目。另外亦可考量以下事項：

- **風險評估：**組織應就法令要求與作業風險進行完整的分析。風險分析結果可用來決定後續改善方向、發展行動計劃、以及分配資源。
- **明確的資料定義：**組織應明確定義個人資料及其涵蓋範圍，並廣泛告知全組織所有人員。此一事項對於跨全球組織非常重要但不易推行，因為不同國家對於何謂個人資料的定義有所不同。例如：薪資、性別、學歷、宗教信仰或是女性婚前娘家的姓氏等，在全球各地對於個資保護的範圍均有可能不同。
- **組織運作與釐清責任：**組織應明確規範由誰負責整體制度的發展、執行、以及有效運作，並確認組織內部的利害關係人。
- **短中期的目標及任務：**組織應確認個資保護

制度的推行成員瞭解且持續推動其目標及任務，例如：資料保護控制機制的建置、利害關係人認知宣導、潛在資料外洩事件的防範等。

- **基本控制的有效性：**組織應確認資料保護相關控制運作的有效性，包括法令規範的基本技術、管理控制，以及判定組織需採用的控制措施。

資料保護制度可協助組織維持法令的持續遵循。稽核是否持續遵循的一種作法為：當組織持續發展時，是否有進行資料保護需求的重新檢視機制。例如，以下情況應當向資料保護專家主動提出諮詢：

- 組織營運模式的改變（如：移轉至消費者市場或是改變行銷策略）
- 資訊科技應用的變動（如：改採用公有雲端服務或改在一個國家集中處理全球員工薪資資料）
- 資料保護法令的變動（應徵詢專家意見，以評估對組織的影響）。

上述事項將有助於稽核人員針對資訊保護制度的有效性及系統性錯誤的防範偵查能力提供合理性的確保。

應注意事項

當稽核跨國組織的資料保護制度時，以下為常見的應注意事項：

- 有更多的商品設備可儲存用戶的個人資料（例如：車用設備、醫療器材等）。該事項可能未列入在組織的檢討範圍內。
- 資料處理委外時，針對第三方廠商的資料保護要求及保證可能是有限的（不論是組織對於第三方廠商的監督不足或是第三方廠商執行工作的品質未達要求）。稽核計劃應當檢視組織與第三方廠商的合約規範內容。由於組織仍需對第三方廠商的工作負起全責，應當對其業務負起監督的責任。
- 企業資源規劃系統(ERP)將個人資料歸為不同的資料分類（例如：客戶資料以及員工資料），而個資法令通常要求員工不能存取與其業務職責無關的個人資料。因此，稽核團隊成員應具有相關的專業技能，能夠針對這些潛在因素加以查核確認。
- 稽核程序中應當針對法令規範的解釋進行討論。團隊成員中的法律專家將有助於其內容及影響結果給予建議。在稽核團隊成員加入個資保護人員（privacy officer）也是可行的做法。可指定個資保護人員稽核與其業務無關的單位，以確保其獨立性。
- 如果沒有結構化的稽核計劃，稽核資料保護制度將會非常複雜。尤其應確認稽核人員與受查者間對於如何達到個資保護有效性的認知是否存在差異。 因此結構化的稽核計劃，為稽核人員出具稽核報告前的重要前置條件。

結論

稽核跨國組織資料保護的有效性受到組織投入的心力所影響。對於法令遵循的查核將有助於瞭解組織近來遵循的概況；而對於資料保護制度的稽核將有助於提昇組織防範資料外洩的能力。

ENDNOTES

1 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." All organizations collect personal data on employees. In addition, depending on the nature of the business, personal data are often collected on customers, suppliers and shareholders. Other examples include patient data and the personal data that companies process on behalf of their customers.*

2 *During their audit work, the authors observed*

only the two general approaches described; there may be other approaches.

3 *Note that "data protection organization" is a general term. It can also be referred to as "privacy organization" or even "information security organization."*

4 *Determining the risk profile and risk appetite is generally part of a risk assessment process. See ISACA, The Risk IT Framework, USA, 2009.*

5 *A recent example of the strong enforcement structure in Germany: "The Data Protection Commissioner's Office (Independent Centre for Privacy Protection [ULD]) calls on all institutions in the federal state of Schleswig-Holstein, Germany to shut down their fan pages on Facebook and remove social plug-ins such as the 'like' button from their web sites." See www.datenschutzzentrum.de/presse/20110819-facebook-en.htm.*

6 *In the UK, the maximum fine under the Data Protection Act is a per-record fine; see www.dotmailer.co.uk/email_marketing_resources/law/penalties_for_noncompliance.aspx. Under US Massachusetts 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth, penalty schemes are based on a formula that multiplies the fine with the number of data subjects affected (people); see www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93i/Section2.*

7 *There are more than 50 individual data protection laws in the world. The most leading laws are related to Europe's Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) and US Massachusetts 201 CMR 17.00. The German Federal Data Protection Act is generally considered to be one of the strictest laws.*

8 *See US Massachusetts 201 CMR 17.00 and the German Federal Data Protection Act.*

9 *See European Committee for Standardization (CEN) Workshop Agreement (CWA) 16112 Self-assessment Framework for Managers, April 2010; CWA 15499-1 Personal Data Protection Audit Framework (EU Directive EC 95/46)—Part I: Baseline Framework, February 2006; and CWA 15499-2 Personal Data Protection Audit Framework (EU Directive EC 95/46)—Part II: Checklists, Questionnaires and Templates for Users of the Framework, February 2006.*

10 *The Institute of Internal Auditors, 2100-5 Legal Considerations in Evaluating Regulatory Compliance Programs, USA, 28 March 2001*