



eBOOK

讓你的組織準備好面對 歐盟通用數據保護條例

(General Data Protection Regulation - GDPR)



企業有許多理由需要保護資料安全：競爭優勢、客戶關係和滿意度、法規需求和審計任務。歐盟立法者在數據安全需求方面邁出新的一步，以另一個角度，即消費者的角度，檢視組織數據的安全。鑑此，歐盟通過通用數據保護條例(General Data Protection Regulation - GDPR)的法令，賦予歐盟公民對其個人資料何時被收集與如何被使用，能夠有更好的管控。歐盟之前就已經通過一些數據保護法令，但GDPR是第一個法令，針對未能保護所收集數據的公司採取重大財務處罰。

此法規將於兩年內，也就是2018年4月開始生效，將會影響任何在歐盟境內做生意和收集歐盟公民個人可識別資訊(Personally Identifiable Information - PII)的組織(無論其總部在何處)。該法令對違規者會產生嚴厲的後果：罰金可高達企業全球年收入的4%或200萬歐元(以金額較大者為準)。

若你的組織已認真執行現行法規，包括PCI DSS、HIPPA或SOX (適用美國境內)，或許多歐盟國家特定數據保護法其中之一，你極有可能已具備良好的數據保護基礎。即使如此，你仍需考慮GDPR的錯綜複雜，特別是GDPR取代現行規章，包括歐盟數據保護法令(European Union Data Protection Directive)。讓情況更複雜的是GDPR讓不同類型的組織難以適應。事實上，它獨特的地方是在組織的風險成長時，增加其責任義務。例如，超過250員工的組織比起低於250員工的組織，需要遵守更嚴謹的規則。

GDPR針對組織在何處及如何存取客戶數據，要求實質的改變，更重要的是組織如何准許其員工、承包商和生意夥伴存取這些數據。此外，它更要求組織在72小時內通報客戶數據的洩漏。這需要將現行安全模式從專注於網路階層的防止數據洩漏演化到即時偵測和補救事件。

GDPR的處罰
最高可達企業
全球年收入的

4%

許多年來，企業都專注於保護網路周邊的安全，作為保護其應用程式和數據的手段。然而，由於憑證的盜用、惡意內部人士行為、和敏感數據擴散儲存於未批准的地點等所造成的許多數據洩露，組織開始瞭解到要減輕這些風險就要對員工、承包商、業務夥伴等在其組織中實施嚴謹的身份管理，並管控這些人可存取的數據、應用程式和系統。當組織採行這些更嚴格的治理控制時，就會發現自身已準備好去面對即將來臨的GDPR要求。

讓你的資料庫井然有序

在新的法規和違規處罰實施之前，現在就是讓你的資料庫井然有序的時候了。組織可採取積極措施保持領先，專注於一些主要的身份治理優先事項：找出敏感數據，了解誰可存取這些數據，並維持對這些數據適當的存取控管。

- 1 辨識出你的敏感數據**
首先，針對你組織內需要依據GDPR加以保護的數據存在於那些地方，建立一個完整圖像。這些數據可能存在於結構化系統中，例如應用程式或資料庫，或以非結構化形式佇留於檔案系統中(例如從應用程式或資料庫輸出的Excel試算表或PDF報告)，或是佇留在協同入口網站(例如SharePoint)，甚或存在於雲端儲存系統中(例如Box或Google Drive)。
- 2 判定誰可存取敏感數據**
再來，了解誰應該有存取客戶數據的權限並依規定存取。這是一個持續進行的程序，而不是一次性的作業。要確保涵蓋所有的應用程式和檔案儲存平台(本機和雲端環境)，這些是你經常儲存客戶數據的地方。
- 3 建立預防性和偵測管控**
使用者應該只能存取其所需的最低限度資源(最小特權)，且對敏感數據的存取需要高度的管制。你需要建立一個治理模型，依據業務需求將應用程式和數據的存取一致化。而這樣的作業功能就是身份和數據存取治理工具能夠幫得上忙的地方，以確保使用者無法執行不當的存取，那麼就可針對使用者的存取進行自動檢視和監控的作業程序。

同時利用身份與數據存取治理

將身份治理平台和數據存取治理解決方案協同作業，你的組織可獲得"誰可對那些數據資料做存取"的完整可見度，並檢視這些使用者如何使用這樣的存取權限。這樣的功能可在數據洩漏情況發生時，以及在存取重新認證和其它安全事件的情況下，幫助你做正確的決定。

一開始，你可能會被GDPR的要求壓得喘不過氣來，特別是不合規時的財務懲罰。然而，利用你安全策略核心的身份治理來保護你組織內對客戶數據的存取，可長遠降低數據洩漏的風險並避免因不合規所導致的罰金。

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint毫無疑問是身份治理領域中的領導者，為全球企業用戶帶來「身份的強大力量」。SailPoint的開放身份平台給予企業進入新市場的力量，擴大員工作業能量，擁抱新的科技與更快速的創新，並於全球規模內展開競爭力 — 安全且充滿信心。本公司開創身份治理市場，並提供以雲端為基礎的整合服務，包括合規控制、配置、密碼管理、單一登入和資料存取治理；這一切皆建立於我們相信身份是一個企業運轉的關鍵。SailPoint的客戶都是全球最大的公司，且涵蓋每一個產業，包括全球前八大銀行、四個前五大健康照護企業、六個前七大產物和意外保險公司、以及前五大製藥公司。