SANS SECURITY AWARENESS

電腦用戶安全意識月刊

GDPR

概觀

您可能已經聽說過一項名為GDPR的新法律，或“通用數據保護條例”。該法律由歐盟制定並於2018年5月25日生效。它適用於任何處理歐盟（EU）居民個人信息的組織，無論該組織所在世界何處。 GDPR要求組織維護任何歐盟居民個人信息的隱私和安全。為了確保符合GDPR，關鍵原則需要理解和實施。

人們有隱私權。組織需要通過限制他們收集和處理的個人數據並保護這些數據來尊重他們的隱私。隱私義務適用於任何信息，不論是通過單獨使用還是與其他信息一起使用，可以識別生活在歐盟的個人。這些信息可以是地址，護照號碼，駕駛執照號碼，財務詳情，生物識別信息，工會會員資格，醫療史，位置數據或與性，宗教或政治取向有關的信息等項目。該規定適用於“自然人”，即有生命的個人。以下是應該遵循的GDPR的一些主要原則：

- 個人的個人資料應以合法，公正和透明的方式處理。
- 人們需要被告知正在收集什麼信息和為了什麼目的而收集。
- 個人數據應按指定的，明確的和合法的目的收集。它不得用於與這些目的相衝突的任何其他原因。
- 個人資料只有在達到該目的所需要的時間內才能保存和處理，並且不超過此時間。
- 個人資料必須保持最新和準確。

人們有權收到他們的數據副本，或者可以要求他們的個人數據不再被使用，或者在某些情況下被完全刪除。

組織必須採取適當的安全措施來保護個人數據免遭意外或非法破壞，丟失，變更或披露。

此外，組織需要確保所有處理個人數據的工作人員都得到適當的培訓，以確保如何保護和保護這些數據。

為保護個人數據而採取的保護措施必須確保適合數據敏感性的保護水平。隨著與數據相關的風險變得越來越大，保護數據的措施和費用也應該越來越大。這些措施應定期審查並酌情更新。紀錄有關隱私和安全決策和措施的記錄，良好的記錄有助於證明符合要求。此外，組織在法律上有義務採取措施（如合同和盡職調查評估）來保護個人數據，包括將其轉移給外部第三方或特別是歐盟以外的當事方。最後，在發生個人數據洩露的情況下，組織應在知悉後72小時內報告違規情況。如果企業未能遵守GDPR，可能會導致其全球收入高達4%的罰款，使GDPR成為全球財務成本最高的全球法規之一。

客座編輯

Brian Honan是位於愛爾蘭都柏林的獨立諮詢網絡安全和數據保護公司BH Consulting的首席執行官。 Brian曾擔任歐洲刑警組織網絡犯罪中心（EC3）的特別顧問，是愛爾蘭第一位CERT的創始人，並擔任多家創新安全公司的諮詢委員會成員。"在www.linkedin.com/in/brianhonan或Twitter @brianhonan可以找到Brian。

參考資料

對個人和組織的GDPR概述: http://gdprandyou.ie
GDPR法規: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
OUCH! 翻譯和檔案: https://www.sans.org/u/D88