SANS SECURITY AWARENESS

全民資訊安全意識月刊

GDPR

概述

您或許聽過一項名為GDPR (General Data Protection Regulation, 通用資料保護規範) 的新法規。這項法規是由歐盟制定並將於2018年5月25日生效。任何處理歐盟民眾個人資料的組織機構, 不論其是否位於歐盟或其他國家, 都適用此法規。GDPR要求全球所有組織機構均須維持歐盟居民的隱私安全。為了確保遵循GDPR, 請務必了解並施行一些重要準則。

由於人們皆享有隱私權, 因此各國組織機構必須有限度地蒐集處理及妥善保護個資以尊重人們的隱私。不論是以直接或間接方式, 只要是足以識別出居住於歐盟地區個人身分的資訊, 組織機構應有義務適當的維護。不論是地址、護照號碼、駕照號碼、財務資料、生物特徵、工會成員、醫療紀錄、定位資料或有關於個人的性生活、宗教及政治傾向皆屬個資。GDPR規範僅及於「自然人」, 也就是活著的個人。以下整理出一些遵行GDPR主要原則:

- 個人資料應以合法、公正及透明的方式加以處理。
- 應告知人們蒐集資料的類別及目的。
- 個資蒐集應有特定的、明確的、合法的目的, 並且不得有任何理由違反。
- 個人資料的保存和處理期限應符合目的之需求, 且不得超過。
- 個人資料應保持更新和正確性。

人們有權利獲得自己的資料複本或要求停止利用並刪除資料。

組織機構必須採取適當的安全措施保護個人資料，以免發生意外或非法的破壞、遺失、變更或揭露。

組織機構需確保所有處理個人資料的員工都有適當的訓練，能夠保護資料安全。

為了保護歐盟民眾個資而採取的保護措施，必須依資料的敏感程度而設有不同等級，且這些措施應定期審查和適時更新；由於伴隨資料而來的風險將不斷升高，相關保護措施所付出的努力和經費也應隨之提高。保有完善紀錄的隱私安全決議與措施將有助突顯組織機構符合GDPR規範要求。此外，將個資傳送至外部第三方，特別是歐盟以外地區時，各組織機構在法律上有義務採取措施（如合約和盡職調查評估）來保護個人資料。最後，如果民眾個資不幸外洩時，組織機構應在知悉後72小時內報告違規情況。如果組織機構無法有效遵行GDPR，可能會導致高達其全球收入4%的罰款，這也使GDPR成為財務成本極高的全球性法規。

德欣寰宇為台灣專業資訊安全顧問公司。我們為客戶提供全方位安全整合解決方案。請至官方網站http://www.tsc-tech.com/或臉書@tsctech了解更多訊息。

客座編輯

Brian Honan在愛爾蘭都柏林的一所網路安全及資料保護獨立顧問公司：BH顧問擔任執行長。Brian同時是歐洲刑警組織網路犯罪中心的特別顧問，也是愛爾蘭第一所CERT的創設者以及數間新創資安公司的顧問。可以在Linkedin: www.linkedin.com/in/brianhonan或推特@brianhonan找到Brian。

參考資料

快速入門，專家解讀GDPR十大重點:	https://www.ithome.com.tw/news/116876
幫助他人自我保護:	https://www.ithome.com.tw/news/116896
OUCH! Translations and Archives:	https://www.sans.org/u/D88

編輯委員會：Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | 翻譯群：黃意雯、宋亞倫、顧君毅、孫權劭、葉力維、莊銘輝