英國資訊委員辦公室（Information Commissioner’s Office，ICO）認定英國電子零售業者Carphone Warehouse違反《Data Protection Act 1998》資料保護法

英國電子零售業者Carphone Warehouse在2015年遭到網路攻擊，造成逾300萬客戶及1000名員工的資料外洩，外洩的資料包括客戶的姓名、地址、電話號碼、出生日期、婚姻狀況及1.8萬名客戶的金融卡資訊。

英國資訊委員辦公室（Information Commissioner’s Office，ICO）認為涉及之個人資料嚴重影響個人隱私，使得個人資料有被誤用的風險。ICO進一步調查後並發現，駭客僅是透過有效的登入憑證，就能藉由WordPress軟體存取系統，此事件亦暴露該組織技術安全措施之不足，因受影響系統中使用的軟件的重要元素已過時，且公司未能執行例行的安全測試。ICO認為，像Carphone Warehouse此類規模龐大的公司，應積極評估其資料安全系統，確保系統穩健而避免類似的攻擊。

據此，ICO判定該公司缺乏妥善的安全措施保障使用者資訊，已嚴重違反《Data Protection Act 1998》資料保護法，判罰40萬英鎊。

從今年5月25日起，隨著GDPR的生效，法律將更加嚴格。對此，ICO亦發布了有用的指導，包括GDPR指南，現在採取的12個步驟和工具包。國家網絡安全中心（NCSC）也為組織為保護自己所採取的步驟提供了有用的指導。

相關連結

- Information Commissioner's Office, Carphone Warehouse fined £400,000 after serious failures placed customer and employee data at risk
- Data Protection Act 1998

你可能會想參加

→ 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會
→ 【已額滿】2023科技研發法制推廣活動—科專個資及反詐騙實務講座
→ 供應鏈資安國際法制與政策趨勢分享會
→ 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
→ 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
→ 商業服務業個資保護宣導說明會
→ 【實體】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
→ 【直播】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
→ 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會
→ 電商零售業法制宣導說明會暨產學研座談會
→ 數位海盜時代來臨–抵禦海上資安威脅的實踐與挑戰
→ 零售業個資保護宣導暨座談會
→ 零售業個資保護及資訊安全教育講習
→ 零售業個資保護及資訊安全教育講習

耿黃瑄
法律研究員 編譯整理

上稿時間：2018年05月

資料來源：

1. Information Commissioner's Office, Carphone Warehouse fined £400,000 after serious failures placed customer and employee data at risk, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/01/carphone-warehouse-fined-400-000-after-serious-failures-placed-customer-and-employee-data-at-risk/ (last visited Apr. 25, 2018).
2. Data Protection Act 1998, http://www.legislation.gov.uk/ukpga/1998/29/contents (last visited Apr. 25, 2018).

文章標籤

個人資料保護與管理 資訊安全

推薦文章